

全国计算机技术与软件专业技术资格（水平）考试参考用书

网络管理员考试全程指导

全国计算机专业技术资格考试办公室推荐

胡钊源 张智勇 施游 主编　　希赛IT教育研发中心 组编

根据2009版大纲编写



清华大学出版社

全国计算机技术与软件专业技术资格（水平）考试参考用书

网络管理员考试全程指导

希赛 IT 教育研发中心　　组编

胡钊源　张智勇　施游　　主编

清 华 大 学 出 版 社
北　京

内 容 简 介

本书由希赛 IT 教育研发中心组织编写，作为全国计算机技术与软件专业技术资格（水平）考试指定参考用书。在对历年考试试题进行分析和总结的基础上，本书着重对考试大纲规定的内容有重点地细化和深化，内容涵盖了最新的网络管理员考试大纲（2009 版）的所有知识点。

阅读本书，就相当于阅读了一本详细的、带有知识注释的考试大纲。准备考试的人员可通过阅读本书掌握考试大纲规定的知识，掌握考试重点和难点，熟悉考试方法、试题形式，试题的深度和广度，以及内容的分布、解答问题的方法和技巧。

本书可作为网络管理员日常工作的参考手册，也可作为计算机专业教师的教学和工作参考书。

本书扉页为防伪页，封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

网络管理员考试全程指导/胡钊源，张智勇，施游主编. —北京：清华大学出版社，2009.10
（全国计算机技术与软件专业技术资格（水平）考试参考用书）
ISBN 978-7-302-21070-2

I. 网…　II. ①胡…　②张…　③施…　III. 计算机网络–工程技术人员–资格考核–自学参考资料　IV. TP393

中国版本图书馆 CIP 数据核字（2009）第 166348 号

责任编辑：柴文强　薛　阳
责任校对：徐俊伟
责任印制：
出版发行：清华大学出版社　　**地　　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185×230　**印　张：**26.25　**防伪页：**1　　**字　数：**601 千字
版　　次：2009 年 10 月第 1 版　　**印　次：**2009 年 10 月第 1 次印刷
印　　数：
定　　价：　　元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　产品编号：033368-01

前　　言

全国计算机技术与软件专业技术资格（水平）考试（以下简称为“软考”）是由国家人力资源和社会保障部、工业和信息化部组织和领导的国家级考试，考试具有很高的权威性，同时也决定了其考试范围的广度和深度都比较大，使许多考生在复习和准备上遇到了很多的难题。虽然国家软考办、希赛 IT 教育研发中心陆续出版了一系列的有针对性的考试辅导教程，为考生复习和备考提供了基础性的帮助，但是，由于考试范围十分广泛，内容量相当大，仍然无法完全满足考生的需求。

1．目的

根据希赛教育网的调查，网络管理员考生最渴望得到的就是一本能全面反映考试大纲内容，同时又比较精简的备考书籍。网络管理员平常工作比较杂，工作压力大，没有多少时间用于学习理论知识，也无暇去总结自己的实践经验，希望能学习一本书籍，从中找到解答试题的捷径。软考的组织者和领导者也希望能有一本书籍帮助考生复习和备考，从而提高考试合格率，为国家信息化建设和信息产业发展培养更多的 IT 人才。

鉴于此，为了帮助广大考生顺利通过网络管理员考试，希赛 IT 教育研发中心组织有关专家，在清华大学出版社的大力支持下，编写和出版了本书，作为网络管理员考试的指定用书。

2．内容

由于考试大纲规定的考试知识点体系庞大，对考生而言，要学习的内容很多，很难把考试大纲规定的知识点全部进行梳理和系统地学习。为此，希赛 IT 教育研发中心组织有关专家对考试大纲和历年考试试题进行了深入的分析，在此基础上编写了本书。就考试中经常出现的一些问题进行归纳和总结，其目的是希望能够压缩所有考试重点和难点知识，而不是囊括所有考试知识点。其结果是让读者顺利通过考试，而不是获得满分。

由于编写组成员均为软考第一线的辅导专家，负责和参与了考试大纲的制定、历年的软考辅导、教程编写、软考阅卷等方面的工作，因此，本书凝聚了软考专家的知识、经验、心得和体会，集成了专家们的精力和心血。

古人云：“温故而知新”，又云：“知己知彼，百战不殆”。对考生来说，阅读本书就是一个“温故”的过程，必定会从中获取到新知识。同时，通过阅读本书，考生还可以清晰地把握命题思路，掌握知识点在试题中的变化，以便在网络管理员考试中洞察先机，提高通过的概率。

3．作者

本书由希赛 IT 教育研发中心组编，由胡钊源、张智勇和施游主编，张友生和桂阳审

核了所有稿件。

全书共分为 16 章。第 1、2 章由王勇编写，第 3、4、15 章由施游编写，第 5、6、9、10、12、16 章由胡钊源编写，第 7 章由何玉云编写，第 8 章由黄少年编写，第 9、13 章由张智勇编写，第 11、14 章由桂阳编写。参加组织和审稿工作的还有王冀、谢顺和周泉。

4．致谢

在本书出版之际，要特别感谢全国计算机专业技术资格考试办公室的命题专家们，我们在本书中引用了各级别部分考试原题，使本书能够尽量方便读者的阅读。同时，本书在编写的过程中参考了许多高水平的资料和书籍（详见参考文献列表），在此，我们对这些参考文献的作者表示真诚的感谢。

感谢清华大学出版社柴文强老师，他在本书的策划、选题的申报、写作大纲的确定，以及编辑、出版等方面，付出了辛勤的劳动和智慧，给予了我们很多的支持和帮助。

感谢希赛教育的网络管理员学员，正是他们的想法汇成了本书的源动力，他们的意见使本书更加贴近读者。

5．交流

由于我们水平有限，且本书涉及的知识点较多，书中难免有不妥和错误之处。我们诚恳地期望各位专家和读者不吝指教和帮助，对此，我们将深为感激。

有关本书的反馈意见，读者可在希赛教育网（http://www. educity.cn）论坛“书评在线”版块中的“希赛 IT 教育研发中心”栏目与我们交流，我们会及时地在线解答读者的疑问。

希赛 IT 教育研发中心

2009 年 7 月

目　　录

第 1 章　计算机科学基础

从历次考试试题来看，计算机科学基础知识是网络管理员考试的一个重点，占上午考试的 4 分左右。根据考试大纲的规定，本章需要考生掌握的考点主要有以下三个方面：

（1）数制及转换：包括二进制、十进制和十六进制等常用数制及其相互转换。

（2）数据的表示：包括数的表示（原码、反码、补码表示，整数和实数的机内表示）、非数值表示（字符和汉字表示、声音表示、图像表示）、校验方法和校验码（奇偶校验、海明校验、CRC 校验）。

（3）数据运算：主要考查计算机中的二进制数运算方法。

1.1　数制及其转换

数据的表示方法有二进制、八进制、十进制和十六进制等。网络管理员考试要求重点掌握这四种进制之间的数据转换方法。

1.1.1　进制的表示

在日常生活中，用十进制来表示数已经广泛被人们所接受。但是由于计算机底层使用的电路硬件通常只能够清晰地表示两种状态，即开和关，或者说高电平和低电平。如果使用十进制，将会使得计算机底层的设计变得过于复杂，而且容易出错，因此通常采用二进制来表示数。

二进制数比较长和比较容易看错，不便于人们进行思考和操作，所以通常采用八进制和十六进制来解决这个问题，八进制和十六进制的表示方法既缩短了二进制数的位数，又保留了二进制数的表达特点。

R 进制，通常说法就是逢 *R* 进 1。可以用的数为 *R* 个，分别是 0，1，2，…，*R*–1。例如八进制数的基数为 8，即可以用到的数码个数为 8，它们是 0，1，2，3，4，5，6，7。二进制数的基数为 2，可用的数码个数为 2，它们是 0 和 1。对于十六进制，它的数码为 0，1，2，3，4，5，6，7，8，9，A，B，C，D，E，F。

为了把不同的进制数分开表示，避免造成混淆，通常采用下标的方式来表示一个数的进制，如十进制数 88 表示为：$(88)_{10}$，八进制数 76 表示为：$(76)_8$。在计算机专业术语的表达中，通常在数字的后面加大写“H”表示十六进制，例如，FCH 就表示十六进制数 FC。

1.1.2 R 进制数与十进制数的转换

对于任意一个 R 进制数，它的每一位数值等于该位的数码乘以该位的权数。权数由一个幂 R^k 表示，即幂的底数是 R，指数为 k，k 与该位和小数点之间的距离有关。当该位位于小数点左边，k 值是该位和小数点之间数码的个数，而当该位位于小数点右边，k 值是负值，其绝对值是该位和小数点之间数码的个数加 1。

例如，八进制数 234.56，其数值可计算如下：

$$234.56=2\times8^2+3\times8^1+4\times8^0+5\times8^{-1}+6\times8^{-2}=128+24+4+5/8+6/64=156.71875$$

又如，二进制数 10100.01 的值可计算如下：

$$10100.01=1\times2^4+1\times2^2+1\times2^{-2}=16+4+0.25=20.25$$

按照上面的表示法，即可计算出 R 进制数转换成十进制数的值。

十进制整数转换成 R 进制数，最常用的是“除以 R 取余法”。例如，将十进制数 94 转换为二进制数：

2 | 94	余	0
2 | 47		1
2 | 23		1
2 | 11		1
2 | 5		1
2 | 2		0
1		1

将所得的余数从低位到高位排列，$(1011110)_2$ 就是 94 的二进制数。

十进制小数转换为 R 进制小数，则采用“乘以 R 取进位法”。例如，将十进制小数 0.43 转换成二进制小数的过程如下（假设要求小数点后取 5 位）：

		0.43×2
高位	0	0.86×2
↓	1	0.72×2
↓	1	0.44×2
↓	0	0.88×2
低位	1	0.76

即转换后的二进制小数为 $(0.01101)_2$。

1.1.3　二进制数与八进制数的转换

将二进制数转换为八进制数，以小数点为分界线，分别从右到左（整数部分）和从左到右（小数部分），将每 3 位二进制数转换为八进制数即可，最后不足 3 位的，则在最高位补 0（整数部分）或最低位补 0（小数部分）。

例如，二进制数 1011110 转换为八进制数，则可以分为 3 段（001，011，110），其对应的八进制数为（1，3，6），因此，$(1011110)_2=(136)_8$。

又如，二进制数 10100.0101 转换为八进制数，则需要在整数部分的最高位补 1 个 0，在小数部分的最低位补 2 个 0，然后分为 4 段（010，100，010，100），其对应的八进制数为（2，4，2，4），因此，$(10100.0101)_2=(24.24)_8$。

相反，将八进制数转换为二进制数，只要将每位八进制数转换为 3 位二进制数即可。

例如，八进制数 56.23 转换为二进制数，因为 5=101，6=110，2=010，3=011，所以 $(56.23)_8=(101110.010011)_2$。

1.1.4　二进制数与十六进制数的转换

将二进制数转换为十六进制数，以小数点为分界线，分别从右到左（整数部分）和从左到右（小数部分），将每 4 位二进制数转换为十六进制数即可，最后不足 4 位的，则在最高位补 0（整数部分）或最低位补 0（小数部分）。

例如，二进制数 1011110 转换为十六进制数，则可以分为 2 段（0101，1110），其对应的十六进制数为（5，E），因此，$(1011110)_2$=5EH。

又如，二进制数 110100.10111 转换为十六进制数，则需要在整数部分的最高位补 2 个 0，在小数部分的最低位补 3 个 0，然后分为 4 段（0011，0100，1011，1000），其对应的十六进制数为（3，4，B，8），因此，$(110100.10111)_2$=34.B8H。

相反，将十六进制数转换为二进制数，只要将每位十六进制数转换为 4 位二进制数即可。

例如，十六进制数 D6.C3H 转换为二进制数，因为 D=1101，6=0110，C=1100，3=0011，所以 D6.C3H=$(11010110.11000011)_2$。

1.2　数据的表示

网络管理员考试要求考生主要掌握数的表示（原码、反码、补码表示法，整数和实数的机内表示）、非数值表示（字符和汉字表示、声音表示、图像表示）、校验方法和校验码（奇偶校验、海明校验、CRC 校验）等知识。

1.2.1 数值的编码表示

本节主要要求掌握原码、反码、补码和移码的概念和特点。

1．原码

原码表示法是在数值前面增加了一位符号位（即最高位为符号位），该位为 0 时表示正数，为 1 时则表示负数，其余各位表示数值的大小。这种方式简单直观，也是最容易理解的。

例如：假设用 8 位表示一个数字，则＋11 的原码是 00001011，–11 的原码是 10001011。其缺点就是原码直接参加运算可能会出现错误的结果。例如：$(1)_{10}+(-1)_{10}=0$。如果直接使用原码，则：$(00000001)_2+(1000001)_2=(10000010)_2$，这样计算的结果是–2，显然出错了。所以，原码的符号位不能直接参与计算，必须和其他位分开，这样会增加硬件的开销和复杂性。

2．反码

反码表示法和原码表示法一样是在数值前面增加了一位符号位（即最高位为符号位），正数的反码与原码相同，负数的反码符号位为 1，其余各位为该数绝对值的原码按位取反。

例如：＋11 的反码是 00001011，–11 的反码为 11110100。

同样对于 $(1)_{10}+(-1)_{10}=0$，如果使用反码，则：$(00000001)_2+(11111110)_2=(11111111)_2$，结果为负 0，而在人们的观念中，0 是不分正负的。反码的符号位可以直接参与计算，而且减法也可以转换为加法运算。注意：用反码进行两数相加时，若最高位有进位，还必须把该进位值加到结果的最低位，才能得到真正的结果，这一操作通称“循环进位”。

3．补码

补码表示法和原码表示法一样是在数值前面增加了一位符号位（即最高位为符号位），正数的补码与原码相同，负数的补码是该数的反码加 1，这个加 1 就是“补”。

例如：＋11 的补码是 00001011，–11 的补码为 11110101。

同样对于 $(1)_{10}+(-1)_{10}=0$，如果使用补码，则：$(00000001)_2+(11111111)_2=(00000000)_2$，直接使用补码计算的结果是正确的。也就是说，补码中 0 是唯一表示的。

在大部分的计算机系统中，数据都使用补码表示，因为采用补码能使符号位与有效值部分一起参加运算，从而简化了运算规则，同时它也使减法运算转换为加法运算，硬件电路只需要设计加法器。

4．移码

移码又称为增码，一般用来表示浮点数的阶码，其定义为：$[X]_{移}=2^n+X\ (-2^n\le X\le 2^n)$

移码的符号表示和补码相反，1 表示正数，0 表示负数。

5．数据的表示范围

对于原码、反码和补码，假设用 n 位表示数据（二进制），则各种表示方法的表示范围如表 1-1 所示。

表 1-1　各种码制所表示数的范围

	定 点 整 数	定 点 小 数
原码	$-(2^{n-1}-1)\sim 2^{n-1}-1$	$-1<X<1$
反码	$-(2^{n-1}-1)\sim 2^{n-1}-1$	$-1<X<1$
补码	$-2^{n-1}\sim 2^{n-1}-1$	$-1\le X<1$

1.2.2　非数值信息的表示

计算机除了处理数值信息以外，还要处理大量的非数值类型的信息，比如字母、汉字、声音、图像等等，然而计算机只能处理二进制数据，当这些非数值类型的信息应用在计算机内，都必须转换为二进制的表现形式。

1．ASCII 码

为了表示英文字母和其他一些符号、控制符，计算机中普遍采用的是 ASCII 码。它使用 7 位代表一个字符，包括了字母的大小写、数字、标点、控制符等。计算机通常使用 8 位一个字节来存储，其高位为 0。表 1-2 列出了全部 128 种字符的 ASCII 码字符编码表。

表 1-2　ASCII 码表

$b_7b_6b_5$ / $b_4b_3b_2b_1$	000	001	010	011	100	101	110	111
0000	NUL	DLE	SPACE	0	@	P		P
0001	SOH	DC1	!	1	A	Q	A	Q
0010	STX	DC2	”	2	B	R	B	R
0011	ETX	DC3	#	3	C	S	C	S
0100	EOT	DC4	$	4	D	T	D	T
0101	ENO	NAK	%	5	E	U	E	U
0110	ACK	SYN	&	6	F	V	F	V
0111	BEL	ETB	’	7	G	W	G	W
1000	BS	CAN	(	8	H	X	H	X
1001	HT	EM	)	9	I	Y	I	Y
1010	LF	SUB	*	:	J	Z	J	Z
1011	VT	ESC	+	;	K	[	K	{
1100	FF	FS	,	<	L	\	L	|
1101	CR	GS	-	=	M	}	M	]

1110	SO	RS	.	>	N	↑	N	~
1111	SI	US	/	?	O	←	o	DEL

2．汉字编码

汉字与西方字符相比，汉字数量大，字型复杂，同音字多，这就给汉字在计算机内部的存储、传输、交换、输入、输出等带来了一系列的问题。为了能直接使用西文标准键盘输入汉字，必须为汉字设计相应的编码，以适应计算机处理汉字的需要。表 1-3 列出了常见的汉字字符编码。

表 1-3　常见的汉字字符编码

编 码 类 型	主 要 类 型
汉字国标码（GB2313-80）	（1）共收集常用汉字 6763 个，其中一级汉字 3755 个，按拼音排序；二级汉字 3008 个，按部首排序；各种图形符号 682 个，共计 7445 个； （2）每个汉字、图形符号都采用两个字节表示，每个字节只使用低 7 位编码。可达到的最大容量是 16 384 个
汉字区位码	（1）将 GB2313-80 中的汉字分为 94 个区，每个区包含 94 个汉字（位），区号和位号来表示汉字； （2）国标码=区位码（十六进制）+2020H
汉字机内码	（1）汉字机内码采用的是两个字节的编码，而每个编码只使用低 7 位，这样就和 ASCII 混淆了，因此在机内表示时将每个字节的最高位置为 1； （2）汉字机内码与国标码的关系为：机内码=国标码+8080H
GB12345-90	（1）繁体字的编码标准，共收录 6866 个汉字，纯繁体有 2200 余个； （2）每个汉字都采用双字节编码
GBK	（1）共收录汉字 21 003 个，符号 883 个，并提供 1894 个造字码位，其特点是简、繁体字融于一库； （2）采用双字节编码
GB18030	（1）涵盖了 27 484 个汉字，繁、简体均处于一个平台； （2）采用单字节、双字节、4 字节混合编码，总编码空间超过 150 万字符

3．声音编码

声音本身是模拟信息，在计算机中表示模拟量必须将模拟量进行数字化，数字化遵循采样定理。

在实践中，通常使用三个参数来表示声音：采样位数、采样频率和声道数。声道有单声道和立体声之分，甚至更多。人能听见的声音的最高频率是 20kHz，根据采样定理，44 100Hz（44kHz）的采样频率能够很好地还原各种声音，而普通人的声带能够达到 4000Hz，所以 8kHz 的采样频率能够满足语言采样的需要。其他采样频率有 11 025Hz

（11kHz）、22 050Hz（22kHz）等，能够适合不同的场景。采样位数是每个采样点采用多少位来保存声音的强度值，采样位数越高，则还原时越精确。如果不采用压缩技术，那么保存声音需要的空间可以这样计算：文件所占容量=（采样频率×采样位数×声道）×时间/8（1 字节=8bit）。

目前主要的音频数据格式如下：

（1）WAVE，扩展名为 WAV：该格式记录声音的波形，故只要采样频率高、采样字节长、机器速度快，利用该格式记录的声音文件就能和原声基本一致，质量非常高，但这样做的代价就是文件太大。

（2）MOD，扩展名 MOD、ST3、XT、S3M、FAR、669 等：该格式的文件里存放乐谱和乐曲使用的各种音色样本，具有回放效果明确，音色种类无限等优点。但它也有一些致命弱点，以至于现在已经逐渐淘汰，目前只有 MOD 迷及一些游戏程序中尚在使用。

（3）Layer-3，扩展名为 MP3：现在最流行的声音文件格式，因其压缩率大，在网络可视电话通信方面应用广泛，但和 CD 唱片相比，音质不能令人非常满意。Layer-3 是 MPEG 标准的一部分，是一种强有力的音频编码方案。Layer-3 在现存的 MPEG-1 和 MPEG-2 国际标准的音频部分上均有定义，简称 MP3（MPEG Audio Layer III）。

（4）Real Audio，扩展名为 RA：这种格式具有强大的压缩量和极小的失真使其在众多格式中脱颖而出。和 MP3 相同，它也是为了解决网络传输带宽资源而设计的，因此主要目标是压缩比和容错性，其次才是音质。

（5）CD Audio 音乐 CD，扩展名为 CDA：唱片采用的格式，又叫“红皮书”格式，记录的是波形流，绝对的纯正、HIFI。但缺点是无法编辑，文件长度太大。

（6）MIDI，扩展名为 MID：作为音乐工业的数据通信标准，MIDI 能指挥各音乐设备的运转，而且具有统一的标准格式，能够模仿原始乐器的各种演奏技巧甚至无法演奏的效果。MIDI 文件是按照 MIDI 标准制成的声音文件。MIDI 文件记录声音的方法与 WAV 完全不同，它并不记录对声音的采集数据，而是记录编曲的音符、音长、音量和击键力度等信息，相当于乐谱。由于 MIDI 文件记录的不是乐曲本身，而是一些描述乐曲演奏过程中的指令，因此它占用的存储空间比 WAV 文件小很多。即使是长达十多分钟的音乐最多也不过几十千字节。

（7）Creative Musical Format，扩展名为 CMF：Creative 公司的专用音乐格式，和 MIDI 差不多，只是音色、效果上有些特色，专用于 FM 声卡，但其兼容性也很差。

4．图像编码

图像也称为位图或点阵图，是指由输入设备捕捉的实际场景画面或以数字化形式存储的任意画面。图像都是由一些排成行列的像素组成的，它除了可以表现真实的照片，也可以表现复杂绘画的某些细节，并具有灵活和富于创造力等特点。

图像的主要指标有分辨率、点距、色彩数（灰度）。

（1）分辨率：可以分为屏幕分辨率和输出分辨率。屏幕分辨率是指每英寸的点阵的行数或列数，这个数值越大，表示就越好。输出分辨率是指每英寸的像素点数，是衡量输出设备的精度，数值越大，质量越好。

（2）点距：指两个像素之间的距离，一般来说，分辨率越高，则像素点距的规格越小，显示效果越好。

（3）深度：图像深度确定彩色图像的每个像素可能有的颜色数，或者确定灰度图像的每个像素可能有的灰度级数。通常，图像深度也指存储每个像素所用的存储器位数，或者说用多少位存储器单元来表示，它也是用来度量图像分辨率的。每个像素颜色或灰度被量化后所占用的存储器位数越多，它能表达的颜色数目就越多，它的深度就越深。

常见的图形/图像文件有以下几种：

（1）BMP（Bit Map Picture）：PC 上最常用的位图格式，有压缩和不压缩两种形式，该格式可表现从 2 位到 24 位的色彩，分辨率也可从 480×320 至 1024×768。该格式在 Windows 环境下相当稳定，在文件大小没有限制的场合中运用极为广泛。

（2）DIB（Device Independent Bitmap）：描述图像的能力基本与 BMP 相同，并且能运行于多种硬件平台，只是文件较大。

（3）PCP（PC Paintbrush）：由 Zsoft 公司创建的一种经过压缩且节约磁盘空间的 PC 位图格式，它最高可表现 24 位图形（图像）。过去有一定市场，但随着 JPEG 的兴起，其地位已逐渐日落终天了。

（4）DIF（Drawing Interchange Format）：AutoCAD 中的图形文件，它以 ASCII 方式存储图形，表现图形在尺寸大小方面十分精确，可以被 CorelDraw、3DS 等大型软件调用编辑。

（5）WMF（Windows Metafile Format）：Microsoft Windows 图元文件，具有文件短小、图案造型化的特点。该类图形比较粗糙，并只能在 Microsoft Office 中调用编辑。

（6）GIF（Graphics Interchange Format）：在各种平台的各种图形处理软件上均可处理的经过压缩的图形格式。缺点是存储色彩最高只能达到 256 种，特别适合于 Web 网页制作，动画制作以及演示文稿等领域。

（7）JPG（Joint Photographics Expert Group）：可以大幅度地压缩图形文件的一种图形格式。对于同一幅画面，JPG 格式存储的文件是其他类型图形文件的 1/10～1/20，而且色彩数最高可达到 24 位，所以它被广泛应用于 Internet 上的 homepage 或 internet 上的图片库。

（8）TIF（Tagged Image File Format）：文件体积庞大，但存储信息量亦巨大，细微层次的信息较多，有利于原稿阶调与色彩的复制。该格式有压缩和非压缩两种形式，最高支持的色彩数可达 16MB。

（9）EPS（Encapsulated PostScript）：用 PostScript 语言描述的 ASCII 图形文件，在 PostScript 图形打印机上能打印出高品质的图形（图像），最高能表示 32 位图形（图像）。

该格式分为 Photoshop EPS 格式、adobeillustrator EPS 格式和标准 EPS 格式，其中后者又可以分为图形格式和图像格式。

（10）PSD（Photoshop Standard）：Photoshop 中的标准文件格式，专门为 Photoshop 而优化的格式。

（11）CDR（CorelDraw）：CorelDraw 的文件格式。另外，CDX 是所有 CorelDraw 应用程序均能使用的图形（图像）文件，是发展成熟的 CDR 文件。

（12）IFF（Image File Format）：用于大型超级图形处理平台，比如 AMIGA 机，好莱坞的特技大片多采用该图形格式处理。图形（图像）效果，包括色彩纹理等逼真再现原景。当然，该格式耗用的内存外存等的计算机资源也十分巨大。

（13）TGA（Tagged Graphic）：是 True vision 公司为其显示卡开发的图形文件格式，创建时期较早，最高色彩数可达 32 位。VDA，PIX，WIN，BPX，ICB 等均属其旁系。

（14）PCD（Photo CD）：由 KODAK 公司开发，其他软件系统对其只能读取。

（15）MPT（Macintosh Paintbrush）或 MAC：Macintosh 机所使用的灰度图形（图像）模式，在 Macintosh Paintbrush 中使用，其分辨率只能是 720×567。

（16）SWF（Flash）：Flash 是 Adobe 公司制定的一种应用于 Internet 的动画格式，它是以矢量图作为基本的图像存储形式的。

除此之外，Macintosh 机专用的图形（图像）格式还有 PNT，PICT，PICT2 等。

1.2.3　校验方法与校验码

信息编码在计算机内传输、存取过程中，难免会出现一些随机性的错误，例如受到外界干扰导致产生了码元错误，例如把“1”码元变成了“0”码元。为了减少和避免这样的错误，提高传输质量，一方面需要从电路、布线等硬件方面采取技术，提高可靠性；另一方面在数据编码上采用某种校验方法与校验码，使得计算机能够自动发现，甚至能自动纠正错误。

常见的信息编码校验方法有奇偶校验法、海明校验法、CRC 校验法等等。

1．奇偶校验法

奇/偶校验是数据传送时采用的一种校正数据错误的一种方式，分为奇校验和偶校验两种。

如果是采用奇校验，在传送每一个数据（一般是 1 个字节）的时候另外附加一位作为校验位，当实际数据中 1 的个数为偶数的时候，这个校验位就是 1。否则，这个校验位就是 0，这样就可以保证传送数据满足奇校验的要求。在接收方收到数据时，将按照奇校验的要求检测数据中 1 的个数，如果是奇数，表示传送正确。否则，表示传送错误。

偶校验的过程和奇校验的过程一样，只是检测数据中 1 的个数为偶数。当实际数据中 1 的个数为偶数的时候，这个校验位就是 0，否则这个校验位就是 1。这样，就可以保证传送数据满足偶校验的要求。在接收方收到数据时，将按照偶校验的要求检测数据中

1 的个数，如果是偶数个 1，表示传送正确。否则，表示传送错误。

2．海明校验法

海明码是奇偶校验的另一种扩充，和奇偶校验不同之处在于海明码采用多位校验码的方式，在信息数据位中合理加入校验位，将码距均匀拉大，校验位中的每一位都对不同的信息数据位进行奇偶校验，通过合理地安排每个校验位对原始数据进行校验位组合，可以达到发现错误，纠正错误的目的。

海明码是利用在信息位为 k 位，增加 r 位冗余位，构成一个 $n=k+r$ 位的码字，然后用 r 个监督关系式产生的 r 个校正因子来区分无错和在码字中的 n 个不同位置的一位错。它必需满足关系式：$2^r \geq n+1$ 或 $2^r \geq k+r+1$。

海明码的编码规则：在一般情况下，校验码会被插入到数据的 1，2，4，8，…，2^n 位置，那么，在数据生成时，按照提供的海明校验方程计算出 b_1，b_2，b_4，…，b_n 各位，在数据校验时，按照海明检验方程进行计算，如果所有的方程式计算都为 0，则表示数据是正确的。如果出现 1 位错误，则至少有一个方程不为 0。海明码的特殊之处在于，只要将①②③三个方程左边计算数据按③②①排列，得到的二进制数值就是该数据中出错的位，例如第 6 位出错，则③②①为 110 为二进制数 6。

当出现两位错误时，这种海明码能够查错，但无法纠错。

3．CRC 校验法

循环冗余检验码简称 CRC 码，由于其实现的原理十分易于用硬件实现，因此广泛地应用于计算机网络上的差错控制。而且由于它采用的是模二除进行验算，因此十分适合于以串行同步方式传送数据块。而 CRC 的考查点主要有 3 个：常见的 CRC 应用标准；计算 CRC 校验码；验算一个加了 CRC 校验的码是否有错误。

（1）常见的 CRC 标准及应用归纳如表 1-4 所示。

表 1-4 常见的 CRC 标准

网 络 协 议	CRC 位	应 用 点
HDLC	CRC16/CRC32	除帧标志位外的全帧
FR（帧中继）	CRC16	除帧标志位外的全帧
ATM	CRC8	帧头校验
以太网（802.3）	CRC32	帧头（不含前导和帧起始符）
令牌总线（802.4）	CRC32	帧头（不含前导和帧起始符）
令牌环（802.5）	CRC32	帧头（从帧控制字段到 LLC）
FDDI	CRC32	帧头（从帧控制字段到 INFO）

（2）计算 CRC 校验码。

在 CRC 码中，编码是由 K 位信息码，加上 R 位的校验码组成。要计算 CRC 校验码，需根据 CRC 生成多项式进行。例如：原始报文为 11001010101，其生成多项式为 $X4+$

*X*3＋*X*＋1。在计算时，是在原始报文的后面若干个 0（等于校验码的位数，而生成多项式的最高幂次就是校验位的位数，即使用该生成多项式产生的校验码为 4 位）作为被除数，除以生成多项式所对应的二进制数（根据其幂次的值决定，得到 11011，因为生成多项式中除了没有 X^2 之外，其他位都有）。然后使用模二除，得到的商就是校验码，如图 1-1 所示。

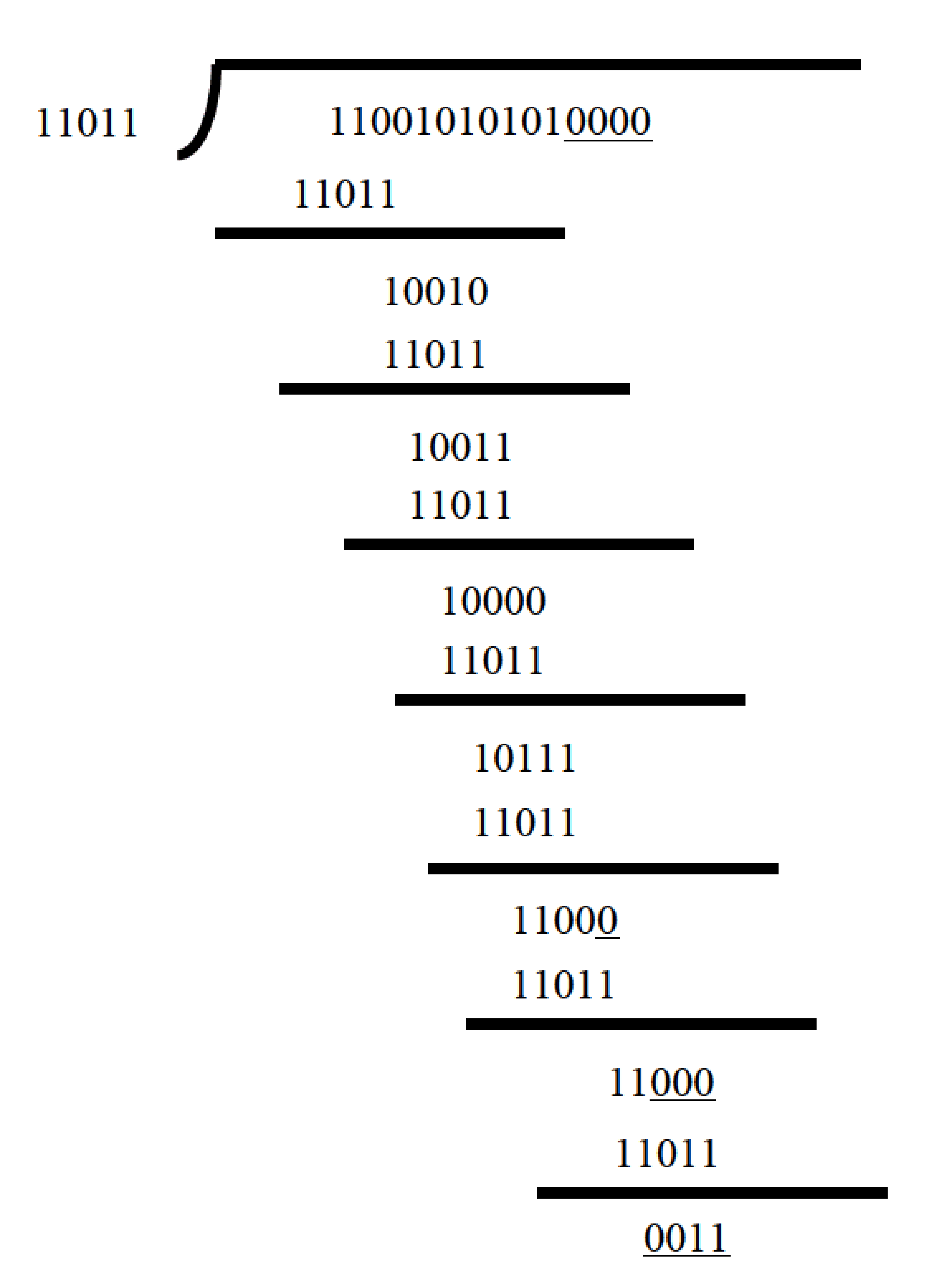


图 1-1　计算 CRC 校验码

然后将 0011 添加到原始报文的后面，就是结果 110010101010011。

（3）检查信息码是否有 CRC 错误。

要想检查信息码是否出现了 CRC 错误的计算很简单，只需用待检查的信息码做被除数，除以生成多项式，如果能够整除就说明没有错误，否则就表示出错了。另外要注意的是，当 CRC 检查出现错误时，它是不会进行纠错的，通常是让信息的发送方重发一遍。

1.3　数据运算

根据考试大纲的要求，在本节知识点中，主要考查计算机中的二进制数运算方法，

其中二进制数的运算可以分为算术运算和逻辑运算。

1．算术运算

二进制数的算术运算比较简单，与十进制算术运算类似，它的基本运算是加法。无论加、减、乘、除运算都可以归结为加法运算。

（1）二进制加法运算规则：0＋0=0；0＋1=1；1＋0=1；1＋1=10（逢二进一）。

（2）二进制减法运算规则：0–0=0；0–1=1（借一当二）；1–0=1；1–1=0。

（3）二进制乘法运算规则：0×0=0；0×1=0；1×0=0；1×1=1。

（4）二进制除法运算规则：0÷0=0；0÷1=0；1÷0=0（无意义）；1÷1=1。

2．逻辑运算

逻辑运算主要包括三种基本运算，分别是逻辑加法（或运算）、逻辑乘法（与运算）和逻辑否定（非运算）。此外，异或运算（半加运算）也很有用。

（1）逻辑加法通常用符号“＋”或“∨”来表示。逻辑加法运算规则如下：

0＋0=0，0∨0=0；

0＋1=1，0∨1=1；

1＋0=1，1∨0=1；

1＋1=1，1∨1=1。

从上式可见，逻辑加法有“或”的意义，因此，也称为逻辑或运算。也就是说，在给定的逻辑变量中，A 或 B 只要有一个为 1，其逻辑加的结果就为 1，只有两者都为 0 时，逻辑加的结果才为 0。

例如，某逻辑电路有两个输入端分别是 X 和 Y，其输出端为 Z。当且仅当两个输入端 X 和 Y 同时为 0 时，输出 Z 才为 0，则该电路输出 Z 的逻辑表达式为 $X+Y$。

（2）逻辑乘法通常用符号“×”或“∧”或“·”来表示。逻辑乘法运算规则如下：

0×0=0，0∧0=0，0·0=0；

0×1=0，0∧1=0，0·1=0；

1×0=0，1∧0=0，1·0=0；

1×1=1，1∧1=1，1·1=1。

不难看出，逻辑乘法有“与”的意义，因此，也称为逻辑与运算。它表示只当参与运算的逻辑变量都同时取值为 1 时，其逻辑乘积才等于 1。只要有一个逻辑变量为 0，其结果就为 0。

例如，用二进制数 0 与累加器 X 的内容进行与运算，并将结果放在累加器 X 中，一定可以完成对 X 的“清 0”操作。

（3）逻辑否运算又称为逻辑非运算。其运算规则为：$\overline{0}=1$，$\overline{1}=0$。

（4）异或运算通常用符号“⊕”表示，其运算规则为：

0⊕0=0，0⊕1=1，1⊕0=1，1⊕1=0。

即两个逻辑变量相异（一个为 0，另一个为 1），结果才为 1。

例如，在进行定点原码乘法运算时，乘积的符号位是被乘数的符号位和乘数的符号位通过异或运算来获得。因为原码的符号位表示数的正负，0 表示正数，1 表示负数。被乘数和乘数都是正数时，值为正数；都为负数时，值也为正数；只有当一个数是正数，另一个数是负数时，值才为负数。

多位数进行逻辑运算时，也是按照“逐位运算”的规则进行的。例如，8 位累加器 A 中的数据为 FCH，若将其与 7EH 相异或，则累加器 A 中的数据为 82H。因为将 FCH 和 7EH 转换为二进制数，得到 11111100 和 01111110，根据异或的运算规则，可以得到 10000010，然后将 10000010 转换成十六进制，得到 82H。

3．移位运算

在前面介绍了二进制数的算术运算中的乘除运算，例如：求 $(1011.11)_2 \times (101)_2$ 的值。利用其运算规则：

```
     1011.11
   ×）101
   ---------
      101111
    000000
   101111
   ---------
   111010.11
```

由上式可见，二进制乘法运算可转换为“加法和移位”运算。在计算机中，实现乘除运算的方案有三种：软件实现，设置专有的乘法、除法器，通过逻辑线路来将乘除运算变换为移位操作。其中以采用移动操作来实现居多。而移位操作主要包括算术移位、逻辑移位和循环移位三种。而移位操作主要包括算术移位、逻辑移位和循环移位三种，如表 1-5 所示。

表 1-5　移位操作的类型

类　型	说　明
算术移位	对象是有符号数，在移位过程中保持操作数的符号位不变，其他各位顺次移动
逻辑移位	对象是无符号数，移位时无须考虑符号位，所有数位统一顺次移动
循环移位	左移出的数放到最右，右移出的数放在最左

例如，对 8 位累加器 A 中的数据 7EH，如果逻辑左移一次，则累加器 A 中的数据为 FCH。因为十六进制数 7EH 转换成二进制为 01111110，根据表 1-5 关于逻辑移位的描述，在移位时不需要考虑符号位，因此，只需将数左移一位，右边空出来的部分补 0，这样就得到二进制数 11111100，再转换成十六进制表示就是 FCH。

在算术移位中，不同码制机器数移位后的空位添补规则如表 1-6 所示。

说明：

（1）机器数为正时，不论左移或右移，空位均添 0。

（2）由于负数的原码其数值部分与真值相同，故在移位时只要使符号位不变，其空

位均添 0。

表 1-6　空位填补规则

	码　制	添补数字
正数	原码、补码、反码	0
负数	原码	0
	补码	左移添 0
		右移添 1
	反码	1

（3）由于负数的反码其各位除符号位外与负数的原码正好相反，故移位后所添的代码应与原码相反，即全部空位添 1。

（4）分析任意负数的补码可发现，当对其由低位向高位找到第一个“1”时，在此“1”左边的各位均与对应的反码相同，而在此“1”右边的各位（包括此“1”在内）均与对应的原码相同，即添 0；右移时因空位出现在高位，则添补的代码应与反码相同，即添 1。

例如，补码 10110100 算术右移 2 位的结果是 11101101。因为最高位为 1，表示是负数，1 作为符号位保持不动，其他各位向右移动 2 位（0110110→01101），这样，左边就空了 2 位，根据表 2-7 的规则，这里应该补 1，则变为 1101101，再加上符号位 1，最后结果为 11101101。

1.4　例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 8 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

若 8 位二进制数能被 4 整除，则其最低 2 位__（1）__。

（1）A. 不可能是 01、00　　B. 只能是 10

C. 可能是 01、00　　D. 只能是 00

例题 1 分析

本题考查的为二进制整除问题，实则可以转换为十进制来计算，其最低 2 位为 00 表示最小的十进制数为 4，能够被 4 整除。

例题 1 答案

（1）D

例题 2

设两个 8 位补码表示的数 $b_7b_6b_5b_4b_3b_2b_1b_0$ 和 $a_7a_6a_5a_4a_3a_2a_1a_0$ 相加时溢出（b_7、a_7

为符号标志），则__（2）__。

（2）A. b_7 与 a_7 的“逻辑或”结果一定为 1
B. b_7 与 a_7 的“逻辑与”结果一定为 0
C. b_7 与 a_7 的“逻辑异或”结果一定为 1
D. b_7 与 a_7 的“逻辑异或”结果一定为 0

例题 2 分析

正数的补码表示与原码相同，即最高符号位为 0，其余为数值位，而负数的补码是由其反码最低位加 1 得来。补码的一个好处就是不同符号位相加不需要通过减法来实现，而直接可以按照二进制加法法则进行，但同符号位的补码相加可能产生溢出，即结果超出了规定的数值范围，使两个正数相加变负数，两个负数相加变正数，即 b_7 与 a_7 的“逻辑异或”结果为 0。例如：89＋67=156，01011001＋01000011=10011100= –28。显然结果是不对的。

例题 2 答案

（2）D

例题 3

欲知八位二进制数（$b_7b_6b_5b_4b_3b_2b_1b_0$）的 b_2 是否为 1，可将该数与二进制数 00000100 进行__（3）__运算，若运算结果不为 0，则此数的 b_2 必为 1。

（3）A. 加　　B. 减　　C. 与　　D. 或

例题 3 分析

这里只要了解二进制数运算的几个概念，很容易分析出，要想结果必定不为 0，并且原数中的第三位是 1，只有“与”运算满足条件，“与”运算只对位进行操作，不涉及到进位，其运算规则为：当参与运算的逻辑变量都同时取值为 1 时，其逻辑乘积才等于 1。只要有一个逻辑变量为 0，其结果就为 0。

例题 3 答案

（3）C

例题 4

汉字机内码与国标码的关系为：机内码 = 国标码 ＋ 8080H。若已知某汉字的国标码为 3456H，则其机内码为__（4）__。

（4）A. B4D6H　　B. B536H　　C. D4B6H　　D. C4B3H

例题 4 分析

根据汉字机内码与国标码的关系：国标码为 3456H 与 8080H 进行相对应的位相加，其中，10～15 分别用 A，B，C，D，E，F。最后计算出来机内码为 B4D6H，其中 H 为进制标识符。

例题 4 答案

（4）A

例题 5

某数值编码为 FFH，若它所表示的真值为–127，则它是用__（5）__表示的；若它所表示的真值为–1，则它是用__（6）__表示的。

（5）A．原码　B．反码　C．补码　D．移码

（6）A．原码　B．反码　C．补码　D．移码

例题 5 分析

原码表示又称符号-数值表示法。正数的符号位用 0 表示，负数的符号位用 1 表示，数值部分保持不变。

反码的符号位表示法与原码相同，即符号 0 表示正数，符号 1 表示负数。与原码不同的是，反码数值部分的形成和它的符号位有关。正数反码的数值和原码的数值相同，而负数反码的数值是原码的数值按位求反。

补码的符号表示和原码相同，0 表示正数；1 表示负数。正数的补码和原码、反码相同，就是二进制数值本身。负数的补码是这样得到的：将数值部分按位取反，再在最低位加 1。补码的补码就是原码。

移码（又称增码）的符号表示和补码相反，1 表示正数；0 表示负数。移码为该数的补码，但符号位相反。常用来表示浮点数的阶码。

–127 原码：1 1111111　　–1 原码：1 0000001

–127 反码：1 0000000　　–1 反码：1 1111110

–127 补码：1 0000001　　–1 补码：1 1111111

–127 移码：0 0000001　　–1 移码：0 1111111

例题 5 答案

（5）A　（6）C

例题 6

__（7）__既具有检错功能又具有纠错功能。

（7）A. 水平奇偶校验　B. 垂直奇偶校验

C. 海明校验　D. 循环冗余校验

例题 6 分析

奇偶校验码是最简单的检错码，奇/偶校验码包括水平奇/偶校验码、垂直奇/偶校验码和水平垂直奇/偶校验码三种编码。由于实现起来比较容易而被广泛采用。

海明码是一种既可检错又可纠错的编码。它的具体原理见本章 1.2.3 节海明校验法。

循环冗余校验：数据通信中应用最广的一种检验差错方法。方法是在发送端用数学方法产生一个循环码，叫做循环冗余检验码。在信息码位之后随信息一起发出。在接收

端也用同样方法产生一个循环冗余校验码。将这两个校验码进行比较，如果一致就证明所传信息无误；如果不一致就表明传输中有差错，并要求发送端再传输。

例题 6 答案

（7）C

例题 7

若信息为 32 位的二进制编码，至少需要加__（8）__位的校验位才能构成海明码。

（8）A. 3　　B. 4　　C. 5　　D. 6

例题 7 分析

根据海明码信息位与校验位间的关系表达式：$2^r \geq n+1$ 或 $2^r \geq k+r+1$。

其中 r 为校验位长度，n 为数据位长度，将 n=32 代入表达式中，可以得出校验位长度为 6。

例题 7 答案

（8）D

例题 8

设机器码的长度为 8，x 为带符号纯小数，y 为带符号纯整数，$[X]_{原}$=11111111，$[Y]_{补}$=11111111，则 x 的十进制真值为__（9）__，y 的十进制真值为__（10）__。

（9）A. 1/128　　B. –1/128　　C. –127/128　　D. 127/128

（10）A. –1　　B. 127　　C. –127　　D. 1

例题 8 分析

带符号的纯小数，符号位是看数字的第一位，0 就是正的，1 就是负的。正数的补码和原码都一样。而负数的补码是把原码除了符号位外全部取反再加上 1。这道题 x 的原码就是 1.1111111。然后再看小数点后 1 所在的位置 n，根据公式 y=（1/2）的 n 次方叠加就行了。这道题小数点后 7 位都是 1，因此是：

其结果是 127/128，再加个负号，就得到 x 的十进制真值了：–127/128。

带符号纯整数，符号位是看数字的第一位，0 就是正的，1 就是负的。正数的补码和原码都一样。而负数的补码是把原码除了符号位外全部取反再加上 1。这里 $[y]_{补}$=11111111，所以 y 的原码是 10000001，则 y 的十进制真值是–1。

例题 8 答案

（9）C　　（10）A

第 2 章　计算机系统基础

一个完整的计算机系统，应该包括两大部分，即计算机硬件系统和计算机软件系统。计算机硬件系统指的是构成计算机的物理设备，而计算机软件系统指的是运行、管理和维护计算机而编制的各种程序、数据和文档的总合。

从历次考试试题来看，计算机系统基础知识是网络管理员考试的一个重点和难点，占上午考试的 7 分左右。根据考试大纲的要求，本章需要考生掌握的考点主要有以下两个方面：

（1）计算机硬件基础知识：包括计算机系统结构和工作原理，CPU 的结构、特征、分类，存储器的结构、特征、分类，I/O 接口、I/O 设备和通信设备。

（2）计算机软件基础知识：包括操作系统的类型、配置操作系统的功能，数据库系统基础知识。

2.1　计算机硬件基础知识

在计算机硬件基础知识方面，希赛教育专家特别提示，本节的主要考点有以下 5 个方面：

（1）计算机组成：包括计算机的基本组成、总线和接口等。

（2）指令系统：包括指令的执行过程、寻址方式。

（3）存储体系：包括内存及编址、内存容量、磁盘等待时间。

（4）中断系统：主要考查中断的基本概念、堆栈。

（5）性能评估：主要考查系统可靠性、容错、时钟频率、机器周期、指令周期等。

2.1.1　计算机组成结构和工作原理

1．计算机组成

在一台计算机中，硬件部分主要由输入系统、输出系统、运算器、控制器和存储器组成。它们之间的合作关系如图 2-1 所示。

（1）运算器：主要负责对信息进行加工处理，从图 2-1 可以看出运算器从内存储器得到需要加工的数据，对数据进行算术运算和逻辑运算，并将最后的结果送回到内存储器中。运算器通常是由 ALU（算术/逻辑单元，包括累加器、加法器等）、通用寄存器（不包含地址寄存器）、多路转换器、数据总线组成。

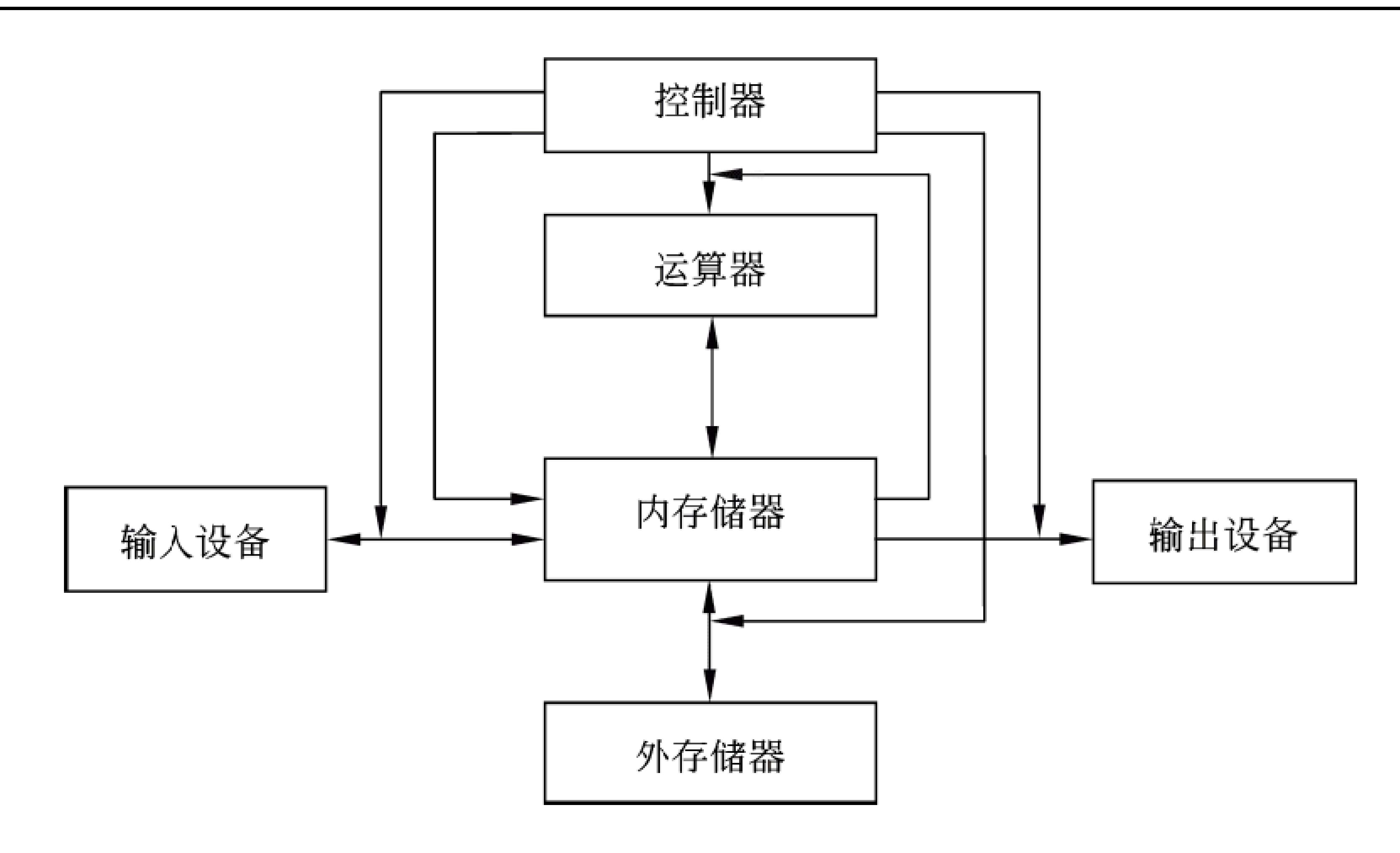


图 2-1　计算机各功能部件之间的合作关系

（2）控制器（Control Unit）：是中央处理器的核心，它控制和协调整个计算机的动作，是分析和执行指令的部件，也是统一指挥并控制计算机各部件协调工作的中心部件，所依据的是机器指令。控制器的组成包含程序计数器（PC）、指令寄存器（IR）、指令译码器、时序部件、微操作控制信号形成部件（PSW）和中断机构。

根据产生微操作控制信号的方式不同，控制器可以分为组合逻辑型、存储逻辑型、组合逻辑与存储逻辑结合型三种。其中存储逻辑型也称为微程序控制型，增加了控制存储器，用来存放控制机器指令执行的微程序。

现在的控制器和运算器被制造在同一块超大规模集成电路中，统称为中央处理器，即 CPU（Central Processing Unit）。

（3）内存储器（Memory 或 Primary storage，简称内存或主存）：直接与运算器相连接，存储容量比较小，速度快，存储现场操作的信息与中间结果，包括机器指令和数据。

（4）外存储器（Secondary storage 或 Permanent storage，简称外存或辅存）：作为内存储器的辅助，其特点是存储容量大，但速度不高，主要是存储需要长期保存和暂时不用的各种信息。

（5）输入设备（Input devices）：将人们的信息形式变换成计算机能接收并识别的信息形式。目前常用的输入设备是键盘、鼠标、扫描仪以及模数转换器等等。

（6）输出设备（Output devices）：把各种计算结果数据或信息以数字、字符、图像、声音等形式表示出来。常见的有显示器、打印机、绘图仪、影像输出系统、语音输出系统等。

（7）总线和接口：计算机总线是一组连接以上各个部件的公共通信线。按总线相对于 CPU 或其他芯片的位置可分为内部总线（Internal Bus）和外部总线（External Bus）两种。在 CPU 内部，寄存器之间和算术逻辑部件 ALU 与控制部件之间传输数据所用的

总线称为内部总线；而外部总线，是指 CPU 与内存 RAM、ROM 和输入/输出设备接口之间进行通信的通路。由于 CPU 通过总线实现程序取指令、内存/外设的数据交换，在 CPU 与外设一定的情况下，总线速度是制约计算机整体性能的最大因素。

2．计算机工作原理

现在的计算机大多数基于冯·诺依曼结构，它的特点是：

（1）采用存储程序的方式，程序和数据放在同一个存储器中，指令和数据都可以送进运算器运算。

（2）数据以二进制数形式表示。

（3）指令由操作码和地址码组成。

（4）指令按照顺序存储，由指令计数器指明当前需要执行指令的地址，通过改变指令计数器来改变程序的流程。

（5）计算机以运算器为中心，输入输出设备和存储器之间的数据传送需要通过运算器。

2.1.2 中央处理器

中央处理器是计算机的控制、运算中心，它主要通过总线和其他设备进行联系，另外在嵌入系统设计中，外部设备也常常直接接到中央处理器的外部 I/O 脚的中断脚上。

中央处理器的类型和品种非常丰富，目前市面上比较流行的是 Intel 公司的酷睿系列和 AMD 公司的弈龙系列，由于都基于冯·诺依曼结构，基本部分组成相似，由运算器和控制器以及寄存器组构成。

1．CPU 的性能特征

计算机系统是一个极复杂的系统，不同的指令系统，不同的体系实现方式，不同数量的硬件，不同的部件组合都对计算机的性能造成这样那样的影响，而且应用对处理器性能的不同方面有不同的要求。这使得处理器性能评价需要综合考虑各方面，全面地衡量处理器的性能。

影响处理器性能的主要因素有：

1）时钟频率

CPU 的时钟频率通常被称为主频，单位是 MHz（或 GHz），通常来说，提高处理器的时钟频率能提高系统的性能，时钟频率仅仅是 CPU 性能表现的一个依据，不能只依靠时钟频率来判断 CPU 性能的高低。

2）外频

CPU 的外频通常也被称为 CPU 的基准频率，单位是 MHz。CPU 的外频决定主板的运行速度。由于 CPU 倍频通常被锁定，因此我们所说的超频一般是指将外频提升达到超频效果。

3）前端总线（FSB）频率

前端总线的速度指的是 CPU 和北桥芯片间总线的速度，更实质性的表示了 CPU 和外界数据传输的速度。“前端总线”（Front Side Bus，FSB）这个名称是由 AMD 在推出 K7 CPU 时提出的概念，一直以来很多教材和资料误认为是 CPU 外频的另一个名称，之所以前端总线与外频这两个概念容易混淆，原因在于在以前一段比较长的时候（主要是 Intel 公司奔腾 4 处理器出现之前和 Intel 公司的奔腾 4 初期），前端总线频率与外频是相同的，因此往往直接称前端总线为外频，最终造成这样的误会。但随着 CPU 技术的发展，前端总线频率需要高于外频，因此采用 Intel 的 QDR（Quad Date Rate）技术来解决这个问题。而 AMD 公司的 CPU 自从 K8 时代以来，前端总线这个名词消失了，取而代之的是 HT（HyperTransport）总线的概念，而如今，AMD K10 的推出，HT 技术也从原来的 1.0 发展到现在的 3.0，传输速率得到极大的提高。

4）倍频

CPU 的时钟频率与外频之间存在着一个比值关系，这个比值就是倍频系数，简称倍频。其公式可表达为：时钟频率=外频×倍频。

5）字长

运算器进行计算的位数称为基本字长，字长越长，处理器能计算的精度就越高，当然处理器的复杂度就越高。因为基本字长增加不但要增加运算器的复杂度，而且需要同时增加寄存器和总线的宽度。

6）数据通路宽度

数据通路宽度指的是数据总线一次所能并行传送的位数，它体现了信息的传送能力，从而影响计算机的有效处理速度。在处理器内部，数据通路的宽度一般是基本字长，而外部总线的数据通路宽度则不一定。如果外部数据通路宽度小于基本字长，那么运算器需要的数据需要多次通过总线从主存传递到处理器内部。

7）缓存

缓存大小也是 CPU 的重要指标之一，位于 CPU 和内存之间的临时存储器，容量比较小，但运行频率非常高，一般是与 CPU 同频工作，缓存容量的大小，直接影响到 CPU 内部读取数据的命中率，但是从 CPU 芯片面积和成本的因素来考虑，缓存一般都很小，又分为一级缓存、二级缓存和三级缓存。

8）指令系统

不同的指令系统对处理器的性能也有非常大的影响。一些处理器对一些专门的应用增加了专门的指令，使得这些处理器在处理这些专门的任务时能“得心应手”。

9）流水线技术

处理器使用流水线技术使不同指令的不同执行部分，能使用不同的处理单元同时执行，比如将一个指令的取址、移码、取操作数、执行、写结果分别由不同的处理单元处理。这样能有效地提高处理器性能。处理器把这些不同的处理单元在硬件上重复，形成多条流水线，以期提高性能。流水线增加了处理器的复杂度，不但处理单元要分开，而

且需要增加流水线管理部分的电路。

除以上九点外，还有很多因素可以影响到 CPU 的性能，比如：制造工艺、核心数等等。

2．指令系统

在计算机中，CPU 都会定义出自己特定的指令系统，不过都遵循着统一的标准格式。指令的基本格式是由操作码和地址码两部分组成的。操作码说明指令的具体功能，地址码通常用来指示操作数的地址。

在指令系统中用来确定如何提供操作数或提供操作数地址的方式称为寻址方式（编址方式）。操作数可以存放在 CPU 中的寄存器（用寄存器名操作）、主存储器（指出存储单元地址）、堆栈（先进后出的存储机制，用栈顶指针 SP 来标出其当前位置）、外存储器或外围设备中。不过在运算时，数据均在主存储器中，操作数可以采用以下几种寻址方式：

（1）立即寻址：直接给出操作数，而非地址。

（2）直接寻址：直接给出操作数地址或所在寄存器号（寄存器寻址）。

（3）间接寻址：给出的是指向操作数地址的地址，称为间接寻址。

（4）变址寻址：给出的地址需与特定的地址值累加从而得出操作数地址，称为变址寻址。

通过采用不同的寻址方式，能够达到缩短指令长度、扩大寻址空间和提高编程灵活性等目的。

例如，某计算机字长为 16 位，运算器为 16 位，有 16 个 16 位通用寄存器，8 种寻址方式，主存容量为 64K 字。指令中地址码由寻址方式字段和寄存器字段组成，采用单字长指令。则要表示 8 种寻址方式需要 3 位，要表示 16 个通用寄存器则需要 4 位，所以地址码一共需要 7 位，而又采用单字长指令，字长为 16 位，因此，操作码的位数就只有 16–7=9 位。也就是说，可以表示的指令种类是 2^9 条，即 512 条。因为每个寄存器是 16 位的，所以，可以表示的地址范围是 2^{16} 字，即 64K 字。

2.1.3 存储器系统

存储器是计算机的重要组成部分，本书中将主要介绍存储器的分类、存储器的性能指标及一些常用的存储器设备。

1．存储器的分类

计算机中，用于存放程序或数据的存储部件按其工作用途分有 CPU 内部寄存器（缓存）、高速缓冲存储器（Cache）、主存储器（内存储器、内存）、辅存（外存储器、外存）。它们的存取速度不一样，从快到慢依次为 CPU 内部寄存器－Cache－内存－辅存。一般来讲，速度越快，成本就会越高。因为成本高，为了节约成本，所以将其容量减小。严格来说，CPU 内部寄存器不算存储系统。因此，在计算机的存储系统体系中，Cache 是

访问速度最快的层次。

按存取方式来分，可分为 RAM（Random Address Memory）和 ROM（Read Only Memory），其中 RAM 是随机存储器，数据可读可写，一旦掉电，数据将消失。随机存储器强调的并非是它的可读可写特性，而是它的“随机”特性，也就是通过地址和数据总线，中央处理器可以“随机”读写存储器的任意某个字节的内容。RAM 有静态和动态两种。最常用的动态 RAM 需要定时刷新电路才能保持数据，而静态 RAM 掉电后信息不丢失，无需刷新过程，所以速度上有优势，而且不需要额外的刷新电路，常作为芯片中的 Cache 使用。而动态 RAM 集成度高、成本低，得到了广泛的应用。而 ROM 是只读存储器，掉电后数据依然保存。这种存储器又可细分为 PROM、EPROM、EEPROM 等类型。在个人计算机中，典型的 ROM 是 BIOS，它里面是个人计算机的硬件检测和引导程序。事实上，有许多种不同类型的存储器，新的产品不断出现，正在打破通常意义上的 RAM 和 ROM 的分界线。既可读可写，又能掉电后仍保持数据的存储器已经出现，被称之为“混合”类型。

2．存储器的性能指标

存储器的性能可以用存取时间、传输率以及存储密度三个指标来表示。

（1）存取时间：指的是从中央处理器发出指令到操作完成的时间。

（2）传输率：或称为数据传输带宽，指单位时间内写入或读取的数据的多少，存取时间越少，传输率越高。

（3）存储密度：单位面积的存储容量。

3．高速缓冲存储器

高速缓冲存储器 Cache 的功能是提高 CPU 数据输入输出的速率，突破所谓的“冯•诺依曼瓶颈”，即 CPU 与存储系统间数据传送带宽限制。高速存储器能以极高的速率进行数据的访问，但因其价格高昂，如果计算机的内存完全由这种高速存储器组成则会大大增加计算机的成本。通常在 CPU 和内存之间设置小容量的高速存储器 Cache。Cache 容量小但速度快，内存速度较低但容量大，通过优化调度算法，系统的性能会大大改善，其存储系统容量与内存相当而访问速度近似 Cache。

Cache 的基本原理：使用 Cache 改善系统性能的依据是程序的局部性原理。依据局部性原理，把内存中访问概率高的内容存放在 Cache 中，当 CPU 需要读取数据时就首先在 Cache 中查找是否有所需内容，如果有，则直接从 Cache 中读取；若没有，再从内存中读取该数据，然后同时送往 CPU 和 Cache。如果 CPU 需要访问的内容大多都能在 Cache 中找到（称为访问命中），则可以大大提高系统性能。

如果以 h 代表对 Cache 的访问命中率（“$1-h$”称为失效率，或者称为未命中率），t_1 表示 Cache 的周期时间，t_2 表示内存的周期时间，以读操作为例，使用“Cache+主存储器”的系统的平均周期为 t_3。则：

$$t_3 = t_1 \times h + t_2 \times (1-h)$$

系统的平均存储周期与命中率有很密切的关系，命中率的提高即使很小也能导致性能上的较大改善。

例如：设某计算机主存的读/写时间为100 ns，有一个指令和数据合一的Cache，已知该Cache 的读/写时间为10 ns，取指令的命中率为98%，取数的命中率为95%。在执行某类程序时，约有1/5指令需要存/取一个操作数。假设指令流水线在任何时候都不阻塞，则设置Cache后，每条指令的平均访存时间约为：

（2%×100ns＋98%×10ns）＋1/5×（5%×100ns＋95%×10ns）= 14.7ns

映射机制：当CPU发出访存请求后，存储器地址先被送到Cache控制器以确定所需数据是否已在Cache中，若命中则直接对Cache进行访问。这个过程称为Cache的地址映射（映像）。在Cache的地址映射中，主存和Cache将均分成容量相同的块（页）。常见的映射方法有直接映射、全相联映射和组相联映射。

直接映射方式以随机存取存储器作为Cache存储器，硬件电路较简单。直接映射是一种多对一的映射关系，但一个主存块只能够复制到Cache的一个特定位置上去。全相联映射使用相联存储器组成的Cache存储器。在全相联映射方式中，主存的每一页可以映射到Cache的任一页。组相联映射是直接映射和全相联映射的折中方案。它将Cache中的块再分成组，通过直接映射方式决定组号，通过全相联映射的方式决定Cache中的块号。在组相联映射方式中，主存中一个组内的块数与Cache的分组数相同。

淘汰算法：当Cache产生了一次访问未命中之后，相应的数据应同时读入CPU和Cache。但是当Cache已存满数据后，新数据必须淘汰Cache中的某些旧数据。最常用的淘汰算法有随机淘汰法、先进先出法（FIFO）和近期最少使用淘汰法（LRU）。其中平均命中率最高的是LRU算法。

写操作：因为需要保证缓存在Cache中的数据与内存中的内容一致，相对读操作而言，Cache的写操作比较复杂，常用的有以下几种方法。

（1）写直达（write through）。当要写 Cache 时，数据同时写回内存，有时也称为写通。

（2）写回（write back）。CPU修改Cache的某一行后，相应的数据并不立即写入内存单元，而是当该行从Cache中被淘汰时，才把数据写回到内存中。

（3）标记法。对Cache中的每一个数据设置一个有效位。当数据进入Cache后，有效位置1；而当CPU要对该数据进行修改时，数据只需写入内存并同时将该有效位清0。当要从Cache中读取数据时需要测试其有效位：若为1则直接从Cache中取数，否则从内存中取数。

4. 磁盘

磁盘是最常见的一种外部存储器，它是由1至多个圆形磁盘组成的，其结构如图2-2所示。

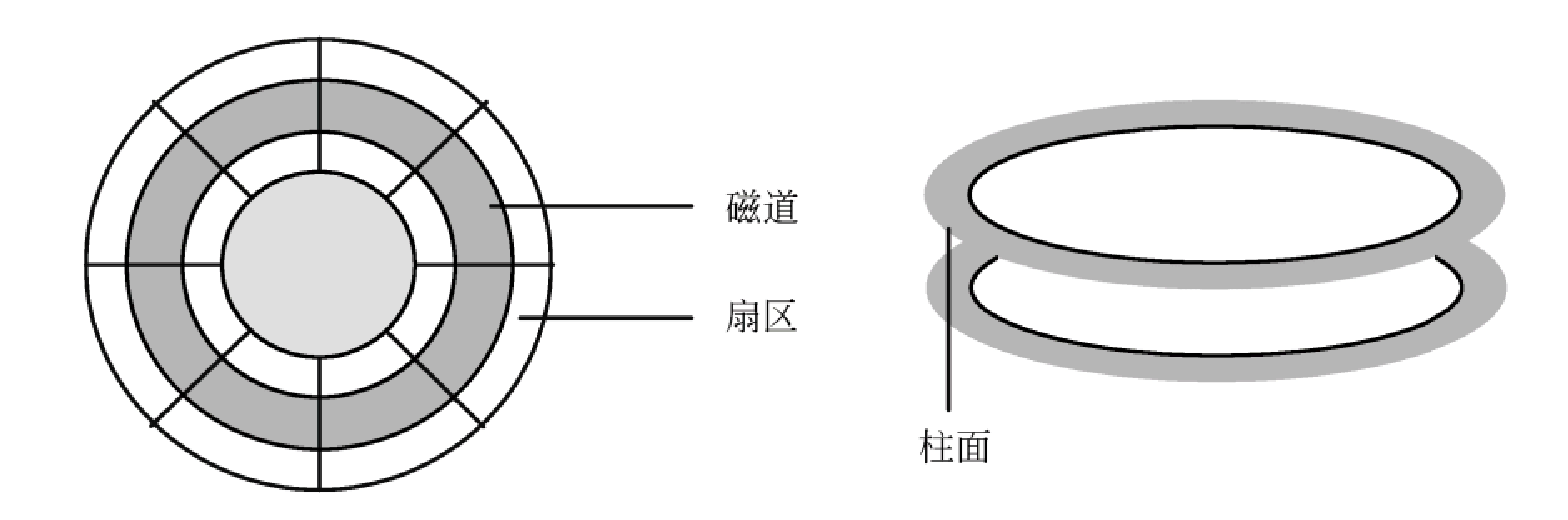


图 2-2　磁盘主要术语示意图

磁盘的常见技术指标如下：

（1）计算磁道数：（外半径–内半径）× 道密度× 记录面数。

说明：硬盘的第一面与最后一面是起保护作用的，一般不用于存储数据，所以在计算的时候要减掉。

（2）非格式化容量=位密度 ×3.14× 最内圈直径 × 总磁道数。

说明：每个磁道的位密度是不相同的，但每个磁道的容量却是相同的。一般来说，0 磁道是最外面的磁道，其位密度最小。

（3）格式化容量 = 每道扇区数 × 扇区容量 × 总磁道数。

（4）平均数据传输速率 = 每道扇区数 × 扇区容量 × 盘片转速。

说明：盘片转速是指磁盘每秒钟转多少转。

（5）存取时间 = 寻道时间 ＋ 等待时间

说明：寻道时间是指磁头移动到磁道所需的时间；等待时间为等待读写的扇区转到磁头下方所用的时间。显然，寻道时间与磁盘的转速没有关系，而是取决于磁盘移动臂的速度。

2.1.4　输入输出系统

输入输出系统即 I/O 系统，它也是整个计算机系统的重要组成部分，本书将主要介绍 I/O 系统的编址方式、输入输出设备及基本的输入输出方式。

1．外设的编址与识别

计算机程序要访问外设，是通过 CPU 访问的输入输出控制器的寄存器。那么对外设就必须加以编址，可以采用以下不同方式对外设加以编址。

1）独立编址

又称独立编址方式。在这种方式下，输入输出地址各主存地址是分开的，有专门的读写控制线以及专门的 I/O 控制指令。I/O 设备的地址空间和存储器地址空间是两个独立的空间。CPU 使用专门的 IN（输入）和 OUT（输出）等 I/O 指令来实现数据传送。工作时，CPU 对指令进行译码（例如，给出 M/IO 信号），区分是存储器读写操作还是

I/O 读写操作。

优点：不占用存储器地址空间。

缺点：需专门的 I/O 指令。

2）统一编址

又称存储器映像编址方式。统一编址中，输入输出地址是主存地址中的一部分，访问输入/输出寄存器与访问主存的方法是一样的。不需要单独的指令。这种方式把每一外设端口视为一个存储单元，统一编排地址，即外设和存储器使用的是同一个地址空间。这样，就可利用访内指令去访问 I/O 端口，而不需要专门的 I/O 指令。CPU 采用存储器读写控制信号（如 MEMR、MEMW），并经地址译码控制来确定是访问存储器还是访问 I/O 设备。

优点：简化指令系统，无需专门的 I/O 指令。

缺点：I/O 端口地址占用了一部分存储器地址空间；I/O 指令码长，执行速度慢。

2．基本的输入输出设备

计算机的输入/输出设备品种繁多，主要有以下几种：

1）纸带机、卡片机

这都是“古代”大型计算机的输入设备，机器指令以打孔等方式存在于纸带、卡片上，由纸带机和卡片机输入计算机，以后人们只能从博物馆见到这些设备。

2）键盘、鼠标

嵌入式系统中键盘往往简化成少数的几个键，和鼠标在本质上没有变化，键盘负责输入字符，鼠标负责指示位置的选择或点取等操作。手写笔是鼠标的扩展，需要识别软件的支持。

3）显示器

嵌入式系统中的显示器往往简化为小屏幕 CD 或数码管，显示器向着越来越大、越来越清晰的方面进步，现在 CRT 显示器仍占主流，但统治地位已经受到了液晶显示器的挑战。触摸屏实际上是显示器和鼠标的结合。

4）外存

外存是主存的辅助和延伸，有软盘、硬盘、光盘存储器、磁带机、闪存等。

5）打印机

打印机将人们需要的结果在纸面上输出。打印机有针打、喷墨、激光打印机。绘图仪是一种特殊的打印机，专门用于大幅的图形精确输出。

6）图形图像摄影输入设备

图形图像摄影输入设备包括扫描仪、数码相机、数字摄像机等。这些设备能把图像摄影等信息输入计算机，极大地丰富了个人计算机在普通家庭的作用。图形图像已经形成了 TWAINS 标准接口，这样软件通过这个标准接口，能同各种不同的图像输入设备进行交互。数字摄像机是通过 USB、1394 或者专用的视频捕捉设备和个人计算机交互。

3．基本的输入输出方式

输入输出系统作为冯·诺依曼体系结构部件之一，输入输出系统是计算机系统中的主机与外部进行通信的系统。它由外围设备和输入输出控制系统两部分组成。外围设备包括输入设备、输出设备和磁盘存储器、磁带存储器、光盘存储器等。从某种意义上也可以把磁盘、磁带和光盘等设备看成一种输入输出设备，所以输入输出设备与外围设备这两个名词经常是通用的。

由于外设的复杂多样性（控制方式，数据传输速率，数据格式也各不相同），并且不断有新的类型的外设出现，很难使用中央处理器来和它们直接打交道。同时这些外设的数据传送速度往往低于系统总线的速度，不适合把它们直接挂在系统总线上。

输入/输出控制器协调和控制数据的输入输出，具体功能有：缓冲锁存数据、地址译码、传递命令、码制转换、电平转换等。

对于工作速度、工作方式和工作性质不同的外围设备，通常要采用不同的输入输出方式。目前常用的基本输入输出方式有三种：

1）程序控制方式

程序控制输入输出方式又称为状态驱动输入输出方式、应答输入输出方式、查询输入输出方式、条件驱动输入输出方式等。图 2-3 表示从键盘输入一个字符到处理机，再把这个字符输出到显示器上的工作过程。用于连接低速外围设备，如终端、打印机等。

2）中断方式

采用中断方式能够完全克服程序控制方式中处理机与外围设备之间不能并行工作的缺点。一般用于连接低速外围设备。

3）直接存储器访问（DMA）方式

直接存储器访问方式又称为 DMA 方式，这种输入输出方式主要用来连接高速外围设备。

例如，磁盘存储器，磁带存储器等。

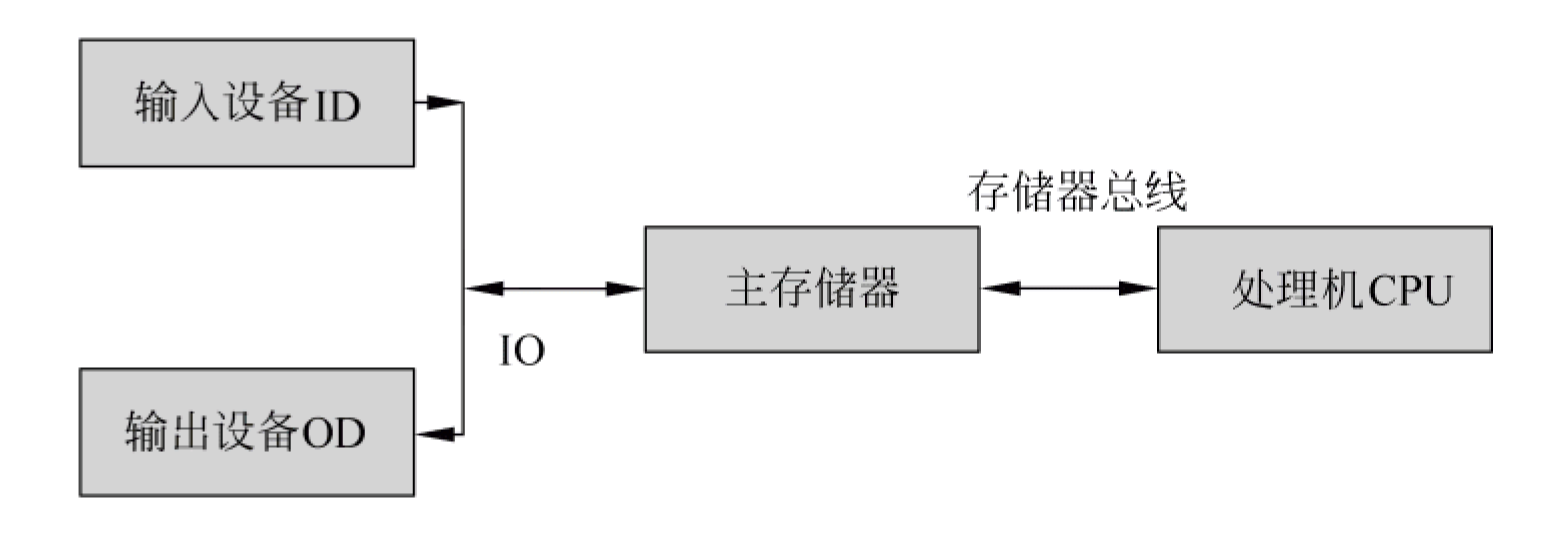


图 2-3　DMA 工作方式

DMA 方式具有如下特点：

（1）外部设备的输入输出请求直接发给主储存器。主存储器既可以被 CPU 访问，也可以被外围设备访问。

（2）不需要做保存现场和恢复现场等工作，从而使 DMA 方式的工作速度大大加快。

（3）在 DMA 控制器中，除了需要设置数据缓冲寄存器、设备状态寄存器或控制寄存器之外，还要设置主存储器地址寄存器，设备地址寄存器和数据交换个数计数器。

（4）在 DMA 方式中，CPU 不仅能够与外围设备并行工作，而且整个数据的传送过程不需要 CPU 的干预。

4．总线技术

总线就是一组进行互连和传输信息（指令、数据和地址）的信号线，它好比连接计算机系统各个部件之间的桥梁。

按总线功能来划分又可分为地址总线、数据总线、控制总线三类。我们通常所说的总线都包括上述三个组成部分，地址总线用来传送地址信息，数据总线用来传送数据信息，控制总线用来传送各种控制信号。

我们通常用总线宽度和总线频率来表示总线的特征。总线宽度为一次能并行传输的二进制位数，即 32 位总线一次能传送 32 位数据，64 位一次能传送 64 位数据。总线频率则用来表示总线的速度。

总线在发展过程中已逐步形成标准化，常见的总线标准有 ISA 总线、PCI 总线、EISA 总线、AGP 总线和 SCSI 总线。

2.2 计算机软件基础知识

根据考试大纲，在计算机软件基础知识方面，希赛教育专家特别提示：计算机软件基础的考点主要包括操作系统、数据库、程序语言、面向对象方法四个方面。

（1）操作系统基础：包括操作系统概念、多道程序设计、存储管理、进程管理、文件管理、作业管理等。

（2）数据库基础：包括数据库概念、数据库模型、数据库功能、关系代数、SQL 语言等。

（3）程序语言基础：包括程序的编译与解释、变量、编程风格、程序控制结构等。

（4）面向对象方法：主要考查面向对象的基本概念和 UML 基础知识。

2.2.1 软件系统基础

计算机软件按其功能可分为应用软件和系统软件两大类。用户与计算机系统各层次之间的关系如图 2-4 所示。

1．系统软件

为了方便用户控制和管理计算机的各种资源，充分发挥计算机系统的效率，围绕计算机系统本身开发的程序系统叫做系统软件。

系统软件具有两大特点：一是通用性，其算法和功能不依赖特定的用户，无论哪个

应用领域都可以使用；二是基础性，其他软件都是在系统软件的支持下开发和运行的。

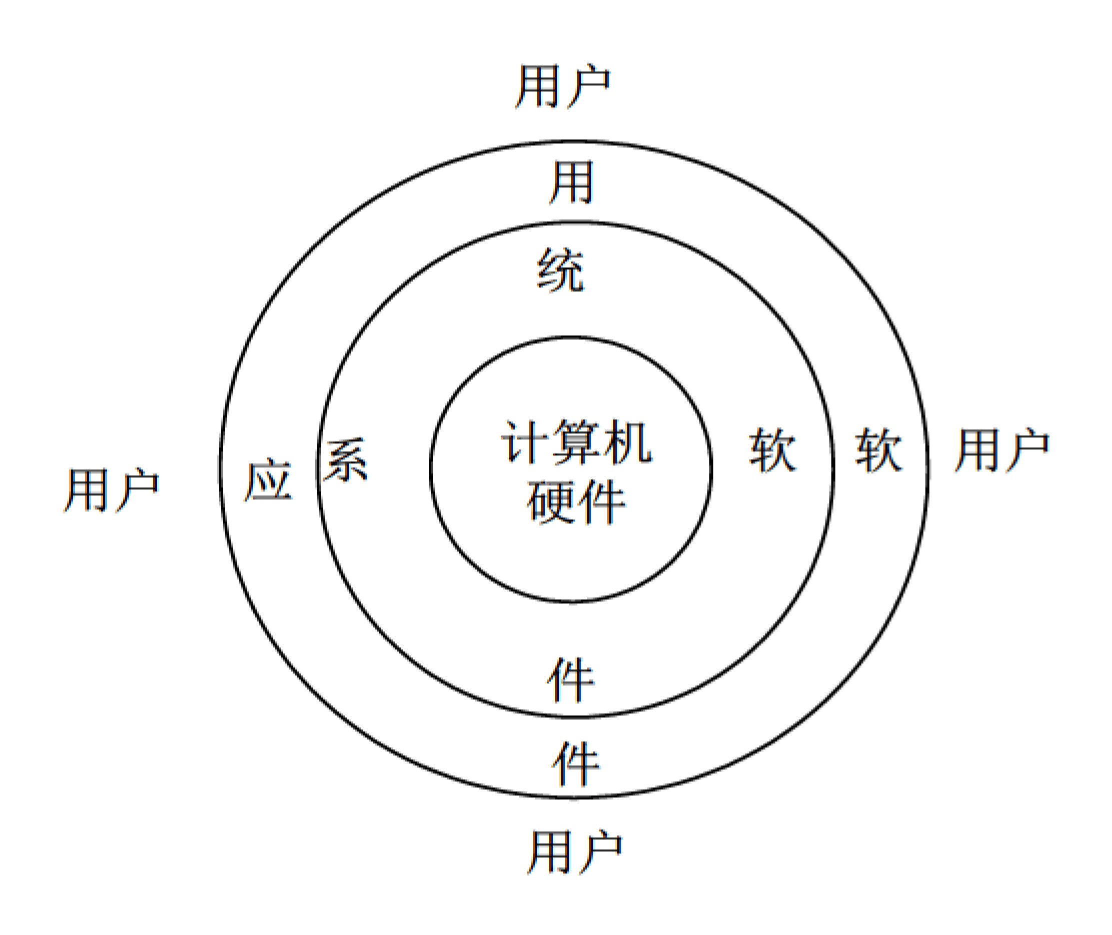


图 2-4　用户与计算机系统各层次之间的关系

系统软件是构成计算机系统必备的软件，如我们经常使用的操作系统（例如 Windows XP、Vista、Linux 和 UNIX 等等）、程序设计语言（例如 C++、Visual Basic、Java 等等）、数据库管理系统（例如 Oracle、My SQL、Microsoft SQL Server、Sybase 等等）。

2．应用软件

软件公司或用户为解决某类应用问题而专门研制的软件称为应用软件。常见的应用软件有文件处理软件（例如 WPS、WORD 等等）、网络应用软件（例如 QQ、MSN、淘宝旺旺等等）、人事管理软件、工程设计绘图软件、办公事务管理软件、图书情报检索软件、医用诊断软件、辅助教学软件、辅助设计软件、网络管理软件、实时控制软件等等。

2.2.2　操作系统基础

操作系统作为计算机系统中的核心系统软件，负责管理和控制计算机系统中的硬件和软件资源，并合理地组织计算机工作流程和有效地利用资源。

操作系统在计算机系统中的地位如图 2-5 所示。

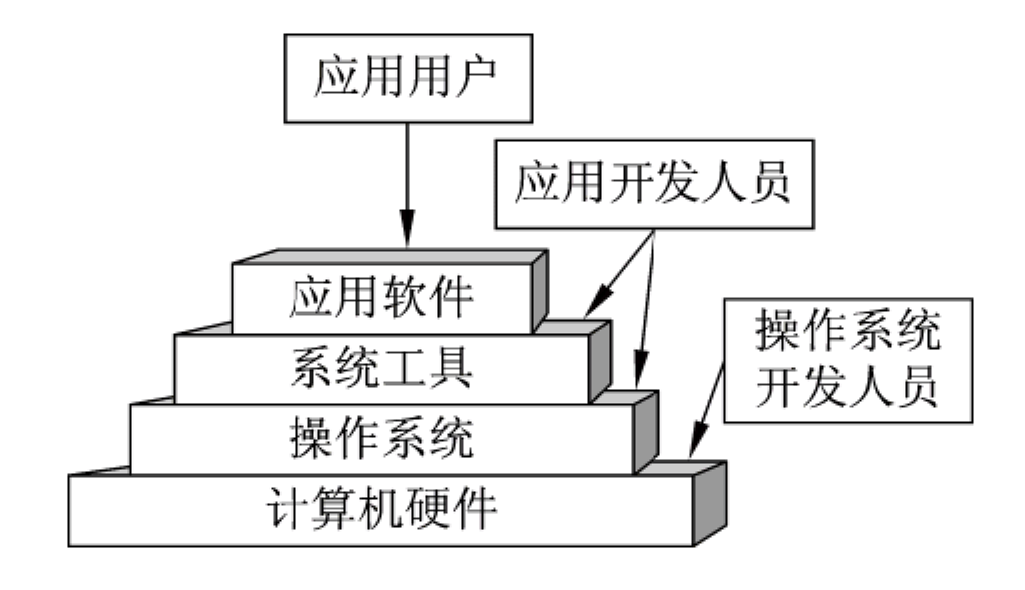


图 2-5　操作系统在计算机系统中的地位

从图 2-5 可知，操作系统在计算机系统中所处的位置是在硬件与其他软件之间的一个特殊位置上，它紧贴系统硬件之上，所有其他软件之下，是其他软件的共同环境。

1．操作系统的类型

根据操作系统在用户界面的使用环境和功能特征的不同，操作系统一般可分为三种基本类型，即批处理系统、分时系统和实时系统。随着计算机体系结构的发展，又出现了许多种操作系统，它们是嵌入式操作系统、个人操作系统、网络操作系统和分布式操作系统。

（1）批处理操作系统（Batch Processing Operating System）。批处理操作系统中，用户的作业分批提交并处理，即系统将作业成批输入系统并暂存在外存中，组成后备作业队列，每次按一定的调度原则从后备作业中选择一个或多个装入主存进行处理，作业完成后退出。这些操作由系统自动实现，在系统中形成了一个自动转接的作业流，当一批作业运行完毕，输出结果后，系统便接收下一批作业。批处理操作系统的特点是：多道和成批处理。

（2）分时操作系统（Time Share Operating System）。一台主机连接若干个终端，每个终端有一个用户在使用。用户交互式地向系统提出命令请求，系统接受每个用户的命令，采用时间片轮转方式处理服务请求，并通过交互方式在终端上向用户显示结果。用户根据上步结果发出下道命令。分时操作系统将 CPU 的时间划分成若干个片段，称为时间片。操作系统以时间片为单位，轮流为每个终端用户服务。每个用户轮流使用一个时间片而使每个用户并不感到有别的用户存在。分时系统具有多路性、交互性、独占性和及时性的特征。多路性指同时有多个用户使用一台计算机，宏观上看是多个人同时使用一个 CPU，微观上是多个人在不同时刻轮流使用 CPU。交互性是指用户根据系统响应结果进一步提出新请求（用户直接干预每一步）。独占性是指用户感觉不到计算机为其他人服务，就像整个系统为他所独占。及时性指系统对用户提出的请求及时响应。

常见的通用操作系统是分时系统与批处理系统的结合。其原则是：分时优先，批处理在后。前台响应需频繁交互的作业，如终端的要求，后台处理时间性要求不强的作业。

（3）实时操作系统（Real Time Operating System，RTOS）。指使计算机能及时响应外部事件的请求在规定的严格时间内完成对该事件的处理，并控制所有实时设备和实时任务协调一致的工作的操作系统。实时操作系统要追求的目标是对外部请求在严格时间范围内做出反应，有高可靠性和完整性。

（4）嵌入式操作系统（Embedded Operating System）。运行在嵌入式系统环境中，对整个嵌入式系统以及它所操作、控制的各种部件装置等资源进行统一协调、调度、指挥和控制的系统软件，并使整个系统能高效地运行。常见的嵌入式操作系统有 Windows CE、Symbian PalmOS 等。

（5）个人计算机操作系统（Personal Computer Operating System）。是一种单用户多任务的操作系统。个人计算机操作系统主要供个人使用，功能强，价格便宜，可以在几乎任何地方安装使用。它能满足一般人操作、学习、游戏等方面的需求。个人计算机操

作系统的主要特点是计算机在某一时间内为单个用户服务；采用图形界面人机交互的工作方式，界面友好；使用方便，用户无须专门学习，也能熟练操纵机器。

（6）网络操作系统（Network Operating System）。网络操作系统是基于计算机网络的，是在各种计算机操作系统上按网络体系结构协议标准开发的软件，包括网络管理、通信、安全、资源共享和各种网络应用。其目标是相互通信及资源共享。

（7）分布式操作系统（Distributed Operating System）。分布式系统是以计算机网络为基础的，由多个分散的处理单元经互联网络的连接而形成的，可以实现分布处理的系统。它的基本特征是处理上的分布，即功能和任务的分布。分布式系统中的每个处理单元既具有高度的自治性，又相互协调，能在系统范围内实现资源管理、动态地分配任务，并能并行地运行分布式程序。在分布式系统上配置的操作系统，称为分布式操作系统。分布式操作系统的所有系统任务可在系统中任何处理机上运行，自动实现全系统范围内任务的分配并自动调度各处理机的工作负载。

2．操作系统的功能

操作系统的功能分成五大部分，即处理机管理、存储管理、文件管理、设备管理和作业管理。这五大部分相互配合，协调工作，实现对计算机系统的资源管理和控制程序的执行，为用户提供方便的使用接口和良好的运行环境。

（1）处理机管理（进程管理）：实质上是对处理机执行时间的管理，即如何将 CPU 真正合理地分配给每个任务进程控制、进程同步、进程通信和调度。

（2）存储管理：实质是对存储空间的管理，主要指对内存的管理、内存分配、内存保护、内存扩充、地址映射、逻辑地址、物理地址的定义。

（3）设备管理：实质是对硬件设备的管理，其中包括对输入输出设备的分配和启动、完成和回收缓冲管理、设备分配、设备处理、设备独立性和虚拟设备。

（4）信息管理（文件管理）：文件存储空间的管理、目录管理、文件的读/写管理和存取控制。

（5）用户接口（作业管理）：命令接口、图形接口、系统调用是操作系统提供给软件开发人员的唯一接口，开发人员可利用它使用系统功能。操作系统核心中都有一组实现系统功能的过程（子程序），系统调用就是对上述过程的调用。包括任务管理、界面管理、人机交互、图形界面、语音控制和虚拟现实等。

3．进程管理

为了描述程序在并发执行时对系统资源的共享，我们需要一个描述程序执行时动态特征的概念，这就是进程。

进程是操作系统中最重要也是最基本的一个概念。掌握这个概念对于理解操作系统实质，对于分析、设计操作系统都具有非常重要的意义。但是迄今为止，对这一概念尚无一个非常确切的、令人满意的、统一的定义。下面是人们从不同的角度对进程所作的解释或所下的定义。

- 进程是可以并发执行的程序在一个数据集合上的运行过程。
- 进程是程序的一次执行过程。
- 进程是可参与并发执行的程序。
- 进程是一个程序及其数据在处理机上执行时所发生的活动。
- 进程是在给定初始状态和内存区域的条件下，可以并发执行的程序的一次执行过程。
- 进程是一个具有一定独立功能的程序，关于某个数据集合的一次运行活动。

一个进程从创建而产生至撤销而消亡的整个生命周期，可以用一组状态加以刻画，为了便于管理进程，可以把进程划分为几种状态，其中常见的有三态模型和五态模型。

1）三态模型

按进程在执行过程中的不同状况至少定义三种不同的进程状态，如图 2-6 所示：

- 运行态：占有处理器正在运行。
- 就绪态：具备运行条件，等待系统分配处理器以便运行。
- 等待态（阻塞态）：不具备运行条件，正在等待某个事件的完成。

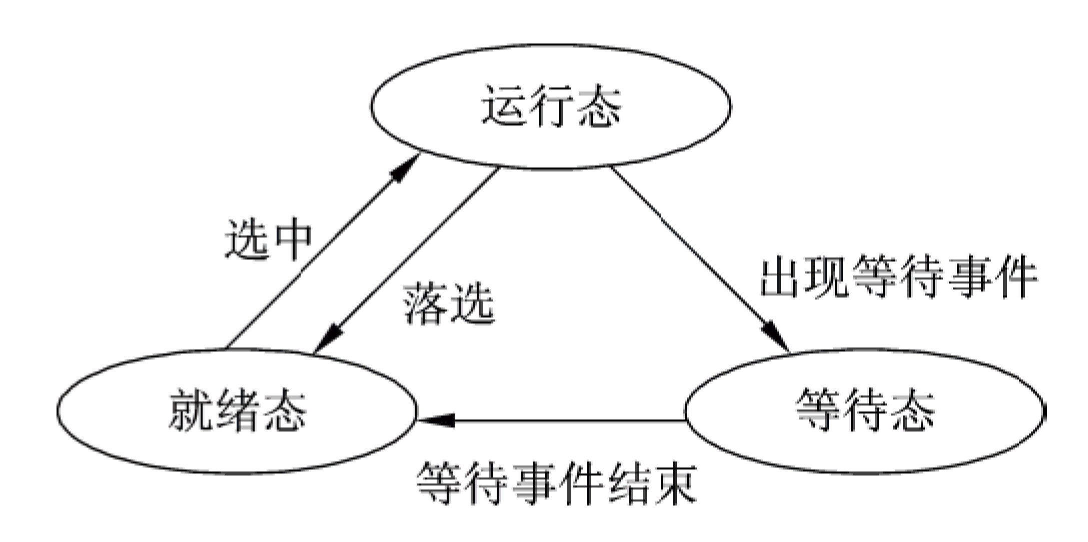


图 2-6　进程三态模型及其状态转换

运行状态的进程将由于出现等待事件而进入等待状态，当等待事件结束之后等待状态的进程将进入就绪状态，而处理器的调度策略又会引起运行状态和就绪状态之间的切换。引起进程状态转换的具体原因如下：

- 运行态→等待态：等待使用资源；如等待外设传输；等待人工干预。
- 等待态→就绪态：资源得到满足；如外设传输结束；人工干预完成。
- 运行态→就绪态：运行时间片到；出现有更高优先权进程。
- 就绪态→运行态：CPU 空闲时选择一个就绪进程。

2）五态模型

五态模型相比于三态模型来说，其进程的状态和转换过程更加复杂，引入了静止就绪态和静止阻塞态的概念，如图 2-7 所示。

4．信号量与 PV 操作

对于本知识点的考查，重点在于理解信号量与 PV 操作的基本概念，能够正确地理解在互斥、同步方面的控制应用，并能够灵活地运用，相对来说是个难点。

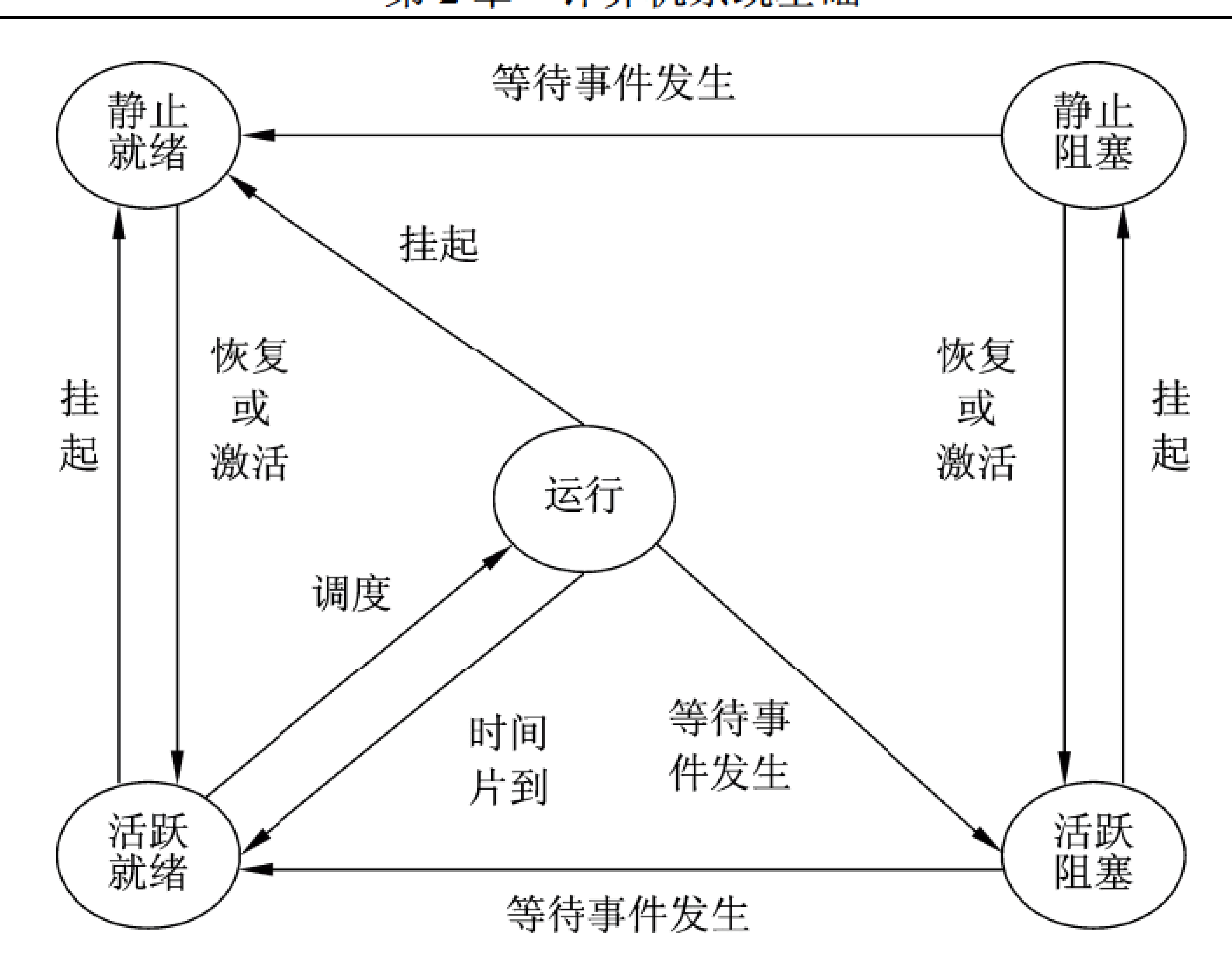


图 2-7　具有挂起功能系统的进程状态及其转换

在操作系统中，进程之间经常会存在互斥（都需要共享独占性资源时）和同步（完成异步的两个进程的协作）两种关系。为了有效地处理这两种情况，荷兰学者 W·Dijkstra 在 1965 年提出信号量和 PV 操作的概念。

信号量：信号量是最早出现的用来解决进程同步与互斥问题的机制，是一种特殊的变量，表现形式是一个整型 S 和一个队列。

P 操作：$S=S-1$，若 $S\geq0$，则执行 P 操作的进程继续执行；若 $S<0$，进程暂停执行，进入等待队列。

V 操作：$S=S+1$，若 $S>0$，则执行 V 操作的进程继续执行；若 $S\leq0$，唤醒等待队列中的一个进程。

1）互斥控制

也就是为了保护共享资源，不让多个进程同时访问这个共享资源，换句话说，就是阻止多个进程同时进入访问这些资源的代码段，这个代码段称为临界区，而这种一次只允许一个进程访问的资源称为临界资源。为了实现进程互斥地进入自己的临界区，代码可以如下所示：

```
P（信号量）
临界区
V（信号量）
```

由于只允许一个进程进入，因此信号量 S 的初值应该为 1。当 $S<0$ 时，其绝对值就是等待使用临界资源的进程数，也就是等待队列中的进程数。而当一个进程从临界区出来时，执行 V 操作（$S=S+1$），如果等待队列中还有进程（$S\leq0$），则调入一个新的进程进

入（唤醒）。

2）同步控制

最简单的同步形式是：进程 A 在另一个进程 B 到达 L2 以前，不应前进到超过点 L1，这样就可以使用程序，如下所示：

```
进程 A                进程 B
…                     …
L1：P（信号量）        L2：V（信号量）
…                     …
```

因此，要确保进程 B 执行 V 操作之前，不让进程 A 的运行超过 L1，就要设置信号量 S 的初值为 0。这样，如果进程 A 先执行到 L1，那么执行 P 操作（$S=S-1$）后，则 $S<0$，就停止执行。直到进程 B 执行到 L2 时，将执行 V 操作（$S=S+1$），唤醒 A 以继续执行。

例如，若某资源的信号量 S 的初值为 2，当前值为–1，则表示系统中有 1 个正在等待该资源的进程。

又如，已知有 n 个进程共享一个互斥段，如果最多允许 m 个进程（$m<n$=同时进入互斥段，则信号量的变化范围是$-(n-m)$～m。因为最多允许 m 个进程同时进入互斥段，说明其初值是 m，而当 n 个进程都进入互斥段时，就有 $n-m$ 个进程在等候，这时信号量的值就是$-(n-m)$，因此信号量的变化范围就是$-(n-m)$～m。

3）生产者与消费者

生产者-消费者是一个经典的问题，它不仅要解决生产者进程与消费者进程的同步关系，还要处理缓冲区的互斥关系，因此通常需要三个信号量来实现，如表 2-1 所示。

表 2-1 生产者-消费者问题

信 号 量	功能类别	功 能 说 明
empty	管理同步	说明空闲的缓冲区数量，最早没有产生东西。因此，其初始值应为缓冲区的最大数
full	管理同步	说明已填充的缓冲区数量，其初始值应为 0
mutex	管理互斥	保证同时只有一个进程在写缓冲区（因此，其初始值应为 1）

如果对缓冲区的读写无须进行互斥控制的话，那么就可以省去 mutex 信号量。

例如，某系统中有一个缓冲区，进程 P1 不断地生产产品送入缓冲区，进程 P2 不断地从缓冲区取出产品消费。假设该缓冲区只能容纳一个产品。进程 P1 与 P2 的同步模型如图 2-8 所示。

这是经典的“生产者-消费者”问题，在本例中，由于“缓冲区只能容纳一个产品”，所以无须对缓冲区的读写进行互斥控制，可以省去 mutex 信号量。因此，可以得知信号量 S1 就是相当于表 2-1 中的 empty，S2 则是相当于表 2-1 中的 full。由于 empty 需说明

空闲的缓冲区数量，而本例中缓冲区数量一开始应该是空闲的，因此应该取值 1。而 full 显然应该取值为 0。

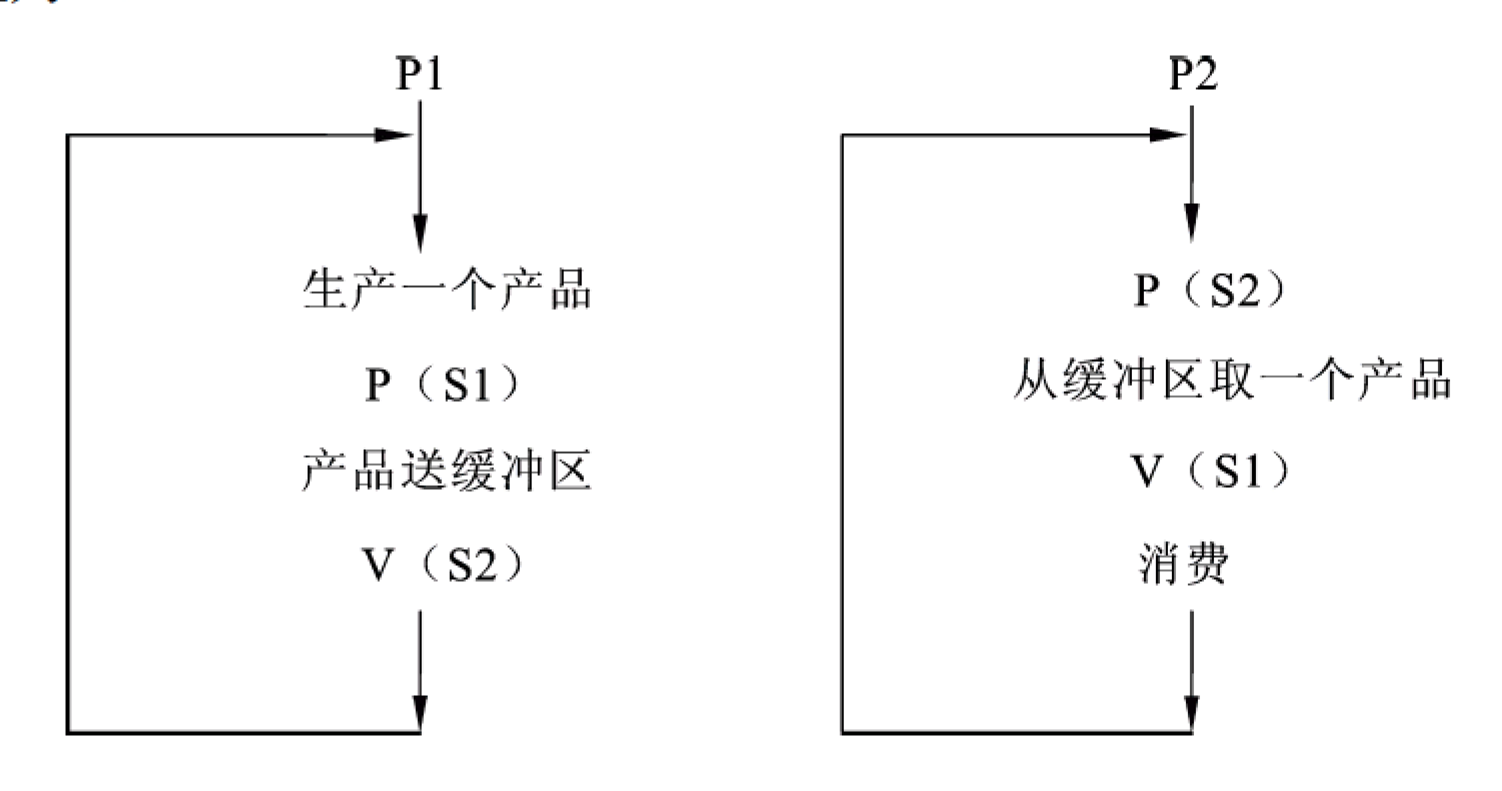


图 2-8　同步模型的例子

4）理解 P、V 操作

信号量与 P、V 操作的概念比较抽象，在历年的考试中总是难倒许多考生，其实主要还是没有能够正确地理解信号量的含义。

信号量与 P、V 操作是用来解决并发问题的，而在并发问题中最重要的是互斥与同步两个关系，也就是说只要有这两个关系存在，信号量就有用武之地。因此，在解题时，应该先从寻找互斥与同步关系开始。这个过程可以套用简单互斥、简单同步、生产者-消费者问题。

通常来说，一个互斥或一个同步关系可以使用一个信号量来解决，但要注意经常会忽略一些隐藏的同步关系。例如，在生产者-消费者问题中，就有两个同步关系，一个判断是否还有足够的空间给生产者存放产物，另一个判断是否有足够的内容让消费者使用。

信号量的初值通常就是表示资源的可用数。而且通常对于初值为 0 的信号量，会先做 V 操作。

在资源使用之前，将会使用 P 操作，在资源用完之后，将会使用 V 操作。在互斥关系中，P、V 操作是在一个进程中成对出现的，而在同步关系中，则 P、V 操作则一定是在两个进程甚至是多个进程中成对出现的。

5. 死锁问题

死锁是指多个进程之间，互相等待对方的资源，而在得到对方资源之前又不释放自己的资源，这样，造成循环等待的一种现象。如果一个进程在等待一个不可能发生的事，则进程就死锁了。如果一个或多个进程产生死锁，就会造成系统死锁。

1）死锁发生的必要条件

互斥条件：即一个资源每次只能被一个进程使用，在操作系统中这是真实存在的情况。

保持和等待条件：有一个进程已获得了一些资源，但因请求其他资源被阻塞时，对已获得的资源保持不放。

不可剥夺条件：有些系统资源是不可剥夺的，当某个进程已获得这种资源后，系统不能强行收回，只能由进程使用完时自己释放。

环路等待条件：若干个进程形成环形链，每个都占用对方要申请的下一个资源。

例如，系统中有 4 个单位的存储器资源，被 n 个进程共享，如果每个进程都要求 i 个单位的存器资源。因为每个进程都需要 i 个存储器资源，如果获得的量小于 i，就会进入等待。如果有 2 个以上进程获得的存储器资源不足 i 个，那么就会进入这样的环路等待，因此只要存储器资源有（n–1）×i 个（或以上）就不会发生死锁，即当 n=2、i=4 时，不可能出现死锁。

2）银行家算法

所谓银行家算法，是指在分配资源之前，先看清楚，当资源分配下去后，是否会导致系统死锁。如果会死锁，则不分配，否则就分配。

对于这些内容，关键在于融会贯通地理解与应用，为了帮助考生更好地理解，下面，我们通过一个例子来说明银行家算法的应用。

假设系统中有三类互斥资源 R1、R2 和 R3，可用资源数分别是 9，8 和 5。在 T0 时刻系统中有 P1、P2、P3、P4 和 P5 五个进程，这些进程对资源的最大需求量和已分配资源数如表 2-2 所示。

表 2-2 进程对资源的最大需求量和已分配资源数

资源 进程	最大需求量			已分配资源数		
	R1	R2	R3	R1	R2	R3
P1	6	5	2	1	2	1
P2	2	2	1	2	1	1
P3	8	0	1	2	1	0
P4	1	2	1	1	2	0
P5	3	4	4	1	1	3

进程按照 P1→P2→P4→P5→P3 序列执行，系统状态安全吗？如果按 P2→P4→P5→P1→P3 的序列呢？

在这个例子中，我们先看一下未分配的资源还有哪些？很明显，还有 2 个 R1 未分配，1 个 R2 未分配，而 R3 全部分配完毕。

按照 P1→P2→P4→P5→P3 的顺序执行时，首先执行 P1，这时由于其 R1、R2 和 R3 的资源数都未分配够，因而开始申请资源，得到还未分配的 2 个 R1，1 个 R2。但其资源仍不足（没有 R3 资源），从而进入阻塞状态，并且这时所有资源都已经分配完毕。因此，后续的进程都无法得到能够完成任务的资源，全部进入阻塞，形成死循环，死锁发

生了。

而如果按照 P2→P4→P5→P1→P3 的序列执行时：

首先执行 P2，它还差 1 个 R2 资源，系统中还有 1 个未分配的 R2，因此满足其要求，能够顺利结束进程，释放出 2 个 R1、2 个 R2、1 个 R3。这时，未分配的资源就是：4 个 R1、2 个 R2、1 个 R3。

然后执行 P4，它还差一个 R3，而系统中刚好有一个未分配的 R3，因此满足其要求，也能够顺利结束，并释放出其资源。因此，这时系统就有 5 个 R1、4 个 R2、1 个 R3……

根据这样的方式推下去，会发现按这种序列可以顺利地完成所有的进程，而不会出现死锁现象。从这个例子中，我们也可以体会到，死锁的四个条件是如何起作用的。只要打破任何一个条件，都不会产生死锁。

3）解决死锁的策略

死锁预防："解铃还需系铃人"，随便破坏导致死锁这任意一个必要条件就可以预防死锁。例如，要求用户申请资源时一次性申请所需要的全部资源，这就破坏了保持和等待条件；将资源分层，得到上一层资源后，才能够申请下一层资源，它破坏了环路等待条件。预防通常会降低系统的效率。

死锁避免：避免是指进程在每次申请资源时判断这些操作是否安全，典型算法是银行家算法。但这种算法会增加系统的开销。

死锁检测：前两者是事前措施，而死锁的检测则是判断系统是否处于死锁状态，如果是，则执行死锁解除策略。

死锁解除：这是与死锁检测结合使用的，它使用的方式就是剥夺。即将某进程所拥有的资源强行收回，分配给其他的进程。

6．存储管理

对于本知识点，主要考查虚拟存储器，特别是页式存储管理。

所谓虚拟存储技术，即在内存中保留一部分程序或数据，在外存（硬盘）中放置整个地址空间的副本。程序运行过程中可以随机访问内存中的数据或程序，但需要的程序或数据不在内存时，就将内存中部分内容根据情况写回外存，然后从外存调入所需程序或数据，实现作业内部的局部对换，从而允许程序的地址空间大于实际分配的存储区域。它在内存和外存之间建立了层次关系，使得程序能够像访问主存一样访问外存，主要用于解决计算机主存储器的容量问题。其逻辑容量由主存和外存容量之和以及 CPU 可寻址的范围来决定，其运行速度接近于主存速度，且成本也不高。可见，虚拟存储技术是一种性能非常优越的存储器管理技术，故被广泛地应用于大、中、小型机器和微型机中。

虚拟存储器允许用户用比主存容量大得多的地址空间来编程，以运行比主存实际容量大得多的程序。用户编程所用的地址称为逻辑地址（又称虚地址），而实际的主存地址则称为物理地址（又称实地址）。每次访问内存时都要进行逻辑地址到物理地址的转换。实际上，超过主存实际容量的那些程序和数据是存放在辅助存储器中的，当使用时再由

辅存调入。地址变换以及主存和辅存间的信息动态调度是硬件和操作系统两者配合完成的。

1）虚拟存储器的分类

虚拟存储器可以分为单一连续分区、固定分区、可变分区、可重定位分区、非请求页式、请求页式、段页式 7 种。

- 单一连续分区。把所有用户区都分配给唯一的用户作业，当作业被调度时，进程全部进入内存，一旦完成，所有主存恢复空闲，因此，它不支持多道程序设计。
- 固定分区。这是支持多道程序设计的最简单的存储管理方法，它把主存划分成若干个固定的和大小不同的分区，每个分区能够装入一个作业，分区的大小是固定的，算法简单，但是容易生成较多的存储器碎片。
- 可变分区。引入可变分区后虽然主存分配更灵活，也提高了主存利用率，但是由于系统在不断地分配和回收中，必定会出现一些不连续的小的空闲区，尽管这些小的空闲区的总和超过某一个作业要求的空间，但是由于不连续而无法分配，产生了碎片。解决碎片的方法是拼接（或称紧凑），即向一个方向（例如向低地址端）移动已分配的作业，使那些零散的小空闲区在另一方向连成一片。分区的拼接技术，一方面是要求能够对作业进行重定位，另一方面系统在拼接时要耗费较多的时间。
- 可重定位分区。这是克服固定分区碎片问题的一种存储分配方法，它能够把相邻的空闲存储空间合并成一个完整的空区，还能够整理存储器内各个作业的存储位置，以达到消除存储碎片和紧缩存储空间的目的。紧缩工作需要花费大量的时间和系统资源。
- 非请求页式。非请求分页式将存储空间和作业的地址空间分成若干个等分部分在分页式，要求把进程所需要的页面全部调入主存后作业方能运行，因此，当内存可用空间小于作业所需的地址空间时，作业无法运行。它克服了分区存储管理中碎片多和紧缩处理时间长的缺点，支持多道程序设计，但不支持虚拟存储。
- 请求页式。非请求分页式将存储空间和作业的地址空间分成若干个等分部分在分页式，当进程需要用到某个页面时将该页面调入主存，把那些暂时无关的页面留在主存外。它支持虚拟存储，克服了分区存储管理中碎片多和紧缩处理时间长的缺点，支持多道程序设计，但是它不能实现对最自然的以段为单位的共享与存储保护（因为程序通常是以段为单位划分的，所以以段为单位最自然）。
- 段页式。这是分段式和分页式结合的存储管理方法，充分利用了分段管理和分页管理的优点。作业按逻辑结构分段，段内分页，内存分块。作业只需部分页装入即可运行，所以支持虚拟存储，可实现动态连接和装配。

现在，最常见的虚存组织有分段技术、分页技术、段页式技术三种。我们把这三种存储组织总结如表 2-3 所示。

表 2-3　常见的虚存组织

项　目	段 式 管 理	页 式 管 理	段页式管理
划分方式	段（不定长） 每个作业一张段表	页（定长） 每个进程一张页表	先将主存分为等长页，每个作业一张段表（通常有一个基号指向它），每段对应一组页表
虚地址	（s，d），即（段号，段内偏移）	（p，d），即（页号，页内偏移）	（s，p，d）即（段号、段内页号、页内偏移）
虚实转换	段表内找出起始地址，然后+段内偏移	页表内找出起始地址，然后+页内偏移	先在段表中找到页表的起始地址，然后在页表中找到起始地址，最后+页内偏移
主要优点	简化了任意增长和收缩的数据段管理，利于进程间共享过程和数据	消除了页外碎片	结合了段与页的优点 便于控制存取访问
主要缺点	段外碎片降低了利用率	存在页内碎片	增长复杂度，增加硬件 存在页内碎片

说明：段内偏移也称为段内地址，页内偏移也称为页内地址。

2）局部性管理

虚拟存储管理的理论基础是程序的局部性原理。

程序局部性原理是指程序在执行时呈现出局部性规律，即在一段时间内，程序的执行仅限于程序的某一部分。相应地，执行所访问的存储空间也局限于某个内存区域。局部性又表现为时间局部性和空间局部性。时间局部性是指如果程序中的某条指令一旦执行，则不久以后该指令可能再次执行。如果某数据被访问，则不久以后该数据可能再次被访问。空间局部性是指一旦程序访问了某个存储单元，则不久之后，其附近的存储单元也将被访问。

根据程序的局部性理论，Denning 提出了工作集理论。工作集是指进程运行时被频繁访问的页面集合。显然只要使程序的工作集全部在内存中，就可以大大减少进程的缺页次数。否则会使进程在运行中频繁出现缺页中断，从而出现频繁的页面调入/调出现象，造成系统性能下降，甚至出现“抖动”。

划分工作集可以按定长时间、或定长页面两种方法进行。当颠簸现象发生时，说明系统负荷过大，通常采用处理器均衡调度，淘汰低优先级进程；另一种是控制缺页率，当缺页率达到上限时，则增加内存分配量；达到下限时，就减少内存分配量。

3）虚存管理

在虚存的管理中涉及载入（调入）、放置（放入分区）和交换（swapping）等问题。

- 调入策略：即何时将一页或一段从外存中调入主存，通常有两种策略，一种是请求调入法，即需要使用时才调入；另一种是先行调入法，即将预计要使用的页/段先行调入主存。

- 放置策略：也就是调入后，放在主存的什么位置，这与实存管理基本上是一致的。
- 置换策略：由于实际主存是小于虚存的，因此可能会发生内存中已满，但需要使用的页不在主存中这一情况（称为缺页中断）。这时就需要进行置换，即将一些主存中的页淘汰到外存，腾出空间给要使用的页，这个过程也称为 Swapping。常见的置换算法如下：
    - 最优算法（OPT）：淘汰不用的或最远的将来才用的页。这是一种理想算法，不可能实现，只是用来作为衡量算法效率的参照物。
    - 随机算法（RAND）：随机淘汰。这种算法开销小，但性能不稳定。
    - 先进先出算法（FIFO）：选择最早调入（也是驻留时间最长）的页。
    - 最近最少使用算法（LRU）：选择离当前时刻最近的一段时间内使用得最少的页。

7. 作业管理

所谓作业，就是用户在一次解题过程中要求计算机系统所做的工作总和。一个作业是指在一次应用业务处理过程中，从输入开始到输出结束，用户要求计算机所做的有关该次业务处理的全部工作。

1）作业的状态

作业由程序、数据和作业说明书三部分组成。作业说明书包括作业基本情况、作业控制和对作业资源要求的描述，它体现用户的控制意图。如预计运行时间、要求的资源情况、执行优先级等。作业从进入系统到运行结束的处理过程，一般要经历提交、后备、运行、完成四个状态。

作业由输入设备进入外存储器（也称输入井）的过程称为提交状态。处于提交状态的作业，其信息正在进入系统。当作业的全部信息进入外存后，系统就为该作业建立一个作业控制块。一个后备作业被作业调度程序选中分配了必要的资源并进入了内存，作业调度程序同时为其建立了相应的进程后，该作业就由后备状态变成了执行状态。当作业正常运行结束，它所占用的资源尚未全部被系统回收时的状态为完成状态。其整个作业的状态及其转换过程如图 2-9 所示。

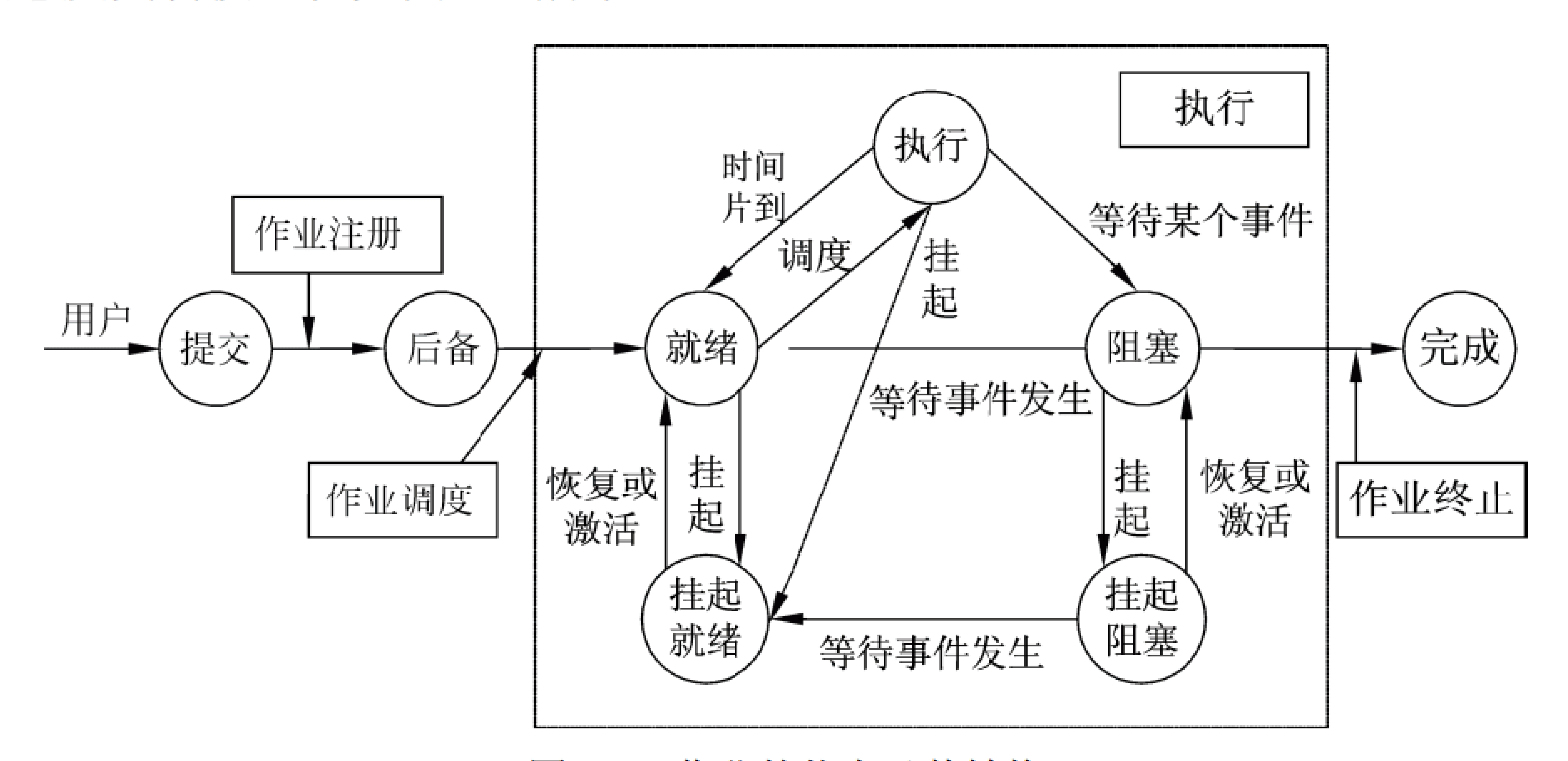


图 2-9 作业的状态及其转换

2）作业的调度

作业调度就是按某种算法从后备作业队列中选择一个作业装入主存开始执行，在作业执行完成后作些善后处理工作。完成这种功能的程序称为作业调度程序。

作业调度的基本功能是检查系统是否满足作业的资源要求，并按一定的算法选取作业，实现作业从后备到运行的状态变换。具体工作是按照一定的算法从后备队列中选出作业后，为其分配内存等必要资源，并创建进程，挂到就绪队列上，使该作业进入运行状态。作业调度也称为宏观调度。

作业调度常用的算法如下：

- 先来先服务（FCFS）调度算法。

先来先服务（FCFS）调度算法按照作业提交的先后次序进行调度，即优先调度在系统中等待时间最长的作业，而不管它要求运行时间的长短。

- 最短作业优先（SJF）调度算法。

最短作业优先（SJF）调度算法选择要求运行时间最短的作业优先调度。

比较上述两种调度算法可以看出，最短作业优先的算法其调度性能要好一点。但是对于长作业可能会产生这种情况，如果不断有短作业进来，则该长作业一直得不到运行机会，这是最短作业优先调度算法的缺点。

- 响应比高者优先（HRN）调度算法。

为了克服上述缺点，可以采用一种称为响应比高者优先的调度算法。响应比 Rp 的定义如下：

$$\text{Rp} = \frac{\text{作业响应时间}}{\text{运行时间（估计值）}} = 1 + \frac{\text{作业等待时间}}{\text{运行时间（估计值）}}$$

所谓响应比高者优先调度算法，就是在每调度一个作业投入运行时，计算后备作业表中每个作业的响应比，挑选响应比最高者。从上述公式可以看出，一个作业的响应比随等待时间的增加而提高，因此在系统中的作业只要它等待足够长的时间，总有可能成为响应比最高者而获得运行机会。

虽然这种算法的调度性能不如最短作业优先调度算法好，但是它既照顾了作业到来的先后顺序，又考虑了要求系统服务时间的长短，所以它是先来先服务算法 FCFS 和短作业优先算法 SJF 的较好折衷。该算法的缺点是较为复杂，每次调度时需对已经到达的作业进行响应比的计算。

8．设备管理

设备管理是对除 CPU、主存和控制台以外的所有设备的管理。这些设备通常称为外部设备或 I/O 设备。

1）设备管理的功能

设备管理是对计算机输入/输出系统的管理。其主要功能是：

（1）提供和进程管理系统的接口。当进程要求设备资源时，该接口将进程要求转达

给设备管理程序。

（2）进行设备分配。按照设备类型和相应的分配算法把设备和其他有关的硬件分配给请求该设备的进程，并把未分配到所请求设备或其他有关硬件的进程放入等待队列。

（3）实现设备和设备、设备和 CPU 等之间的并行操作。

（4）进行缓冲区管理。主要减少外部设备和内存与 CPU 之间的数据速度不匹配的问题，系统中一般设有缓冲区（器）来暂放数据。设备管理程序负责进行缓冲区分配、释放及有关的管理工作。

要注意的是，在 UNIX 系统中，是把输入/输出设备当做特殊文件来处理的。

2）设备驱动程序

设备驱动程序是一种可以使计算机和设备通信的特殊程序，可以说相当于硬件的接口，操作系统只有通过这个接口，才能控制硬件设备的工作，假如某设备的驱动程序未能正确安装，便不能正常工作。正因为这个原因，驱动程序在系统中所占的地位十分重要，一般当操作系统安装完毕后，便是安装硬件设备的驱动程序。

驱动程序的任务是首先将硬件本身的功能告诉操作系统，接下来是完成硬件设备电子信号与操作系统及软件的高级编程语言之间的互相翻译。当操作系统需要使用某个硬件时，比如，让声卡播放音乐，它会先发送相应指令到声卡驱动程序，声卡驱动程序接收到后，马上将其翻译成声卡才能听懂的电子信号命令，从而让声卡播放音乐。

因此，驱动程序处在操作系统和硬件之间，与上层软件无关。

3）虚拟设备

SPOOLING（Simultaneous Peripheral Operation On Line）的意思是外部设备同时联机操作，又称为假脱机输入输出操作，采用一组程序或进程模拟一台 I/O 处理器。SPOOLING 系统的组成如图 2-10 所示。

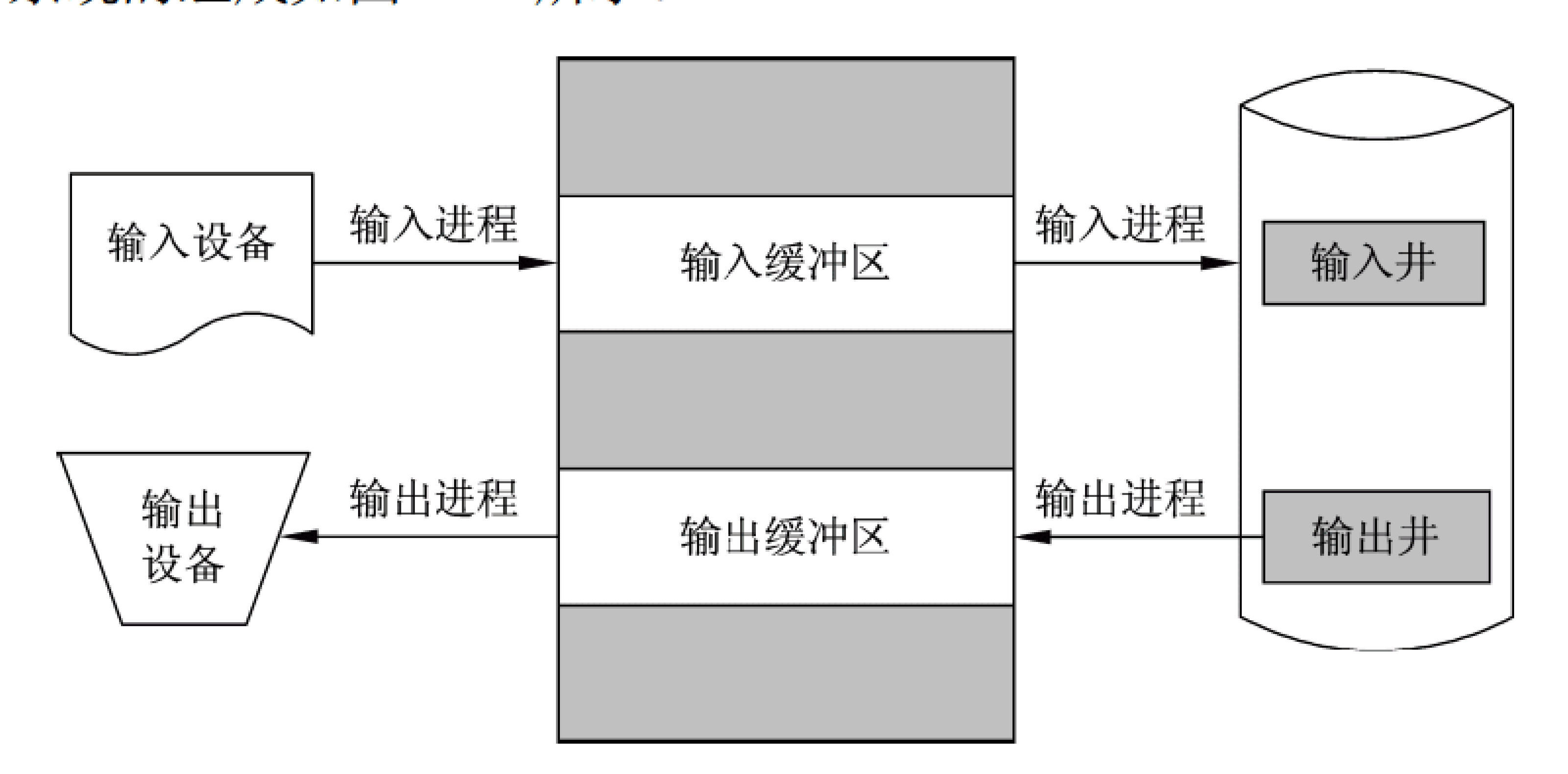


图 2-10 SPOOLING 系统示意图

该技术利用了专门的外围控制机将低速 I/O 设备上的数据传送到高速设备上，或者相反。但是当引入多道程序后，完全可以利用其中的一道程序来模拟脱机输入时的外围

控制机的功能，把低速的 I/O 设备上的数据传送到高速磁盘上；再利用另一道程序来模拟脱机输出时的外围控制机的功能，把高速磁盘上的数据传送到低速的 I/O 设备上。这样便可以在主机的控制下实现脱机输入、输出的功能。此时的外围操作与 CPU 对数据的处理同时进行，将这种在联机情况下实现的同时外围操作称为 SPOOLING，或称为假脱机操作。

采用假脱机技术，可以将低速的独占设备改造成一种可共享的设备，而且一台物理设备可以对应若干台虚拟的同类设备。SPOOLING 系统必须有高速、大容量并且可随机存取的外存（如磁盘或磁鼓）支持。

9．文件管理

信息是计算机系统中的重要资源。文件系统是负责对信息的组织、存储和访问。从资源观点来看，文件系统是操作系统对软件资源的管理，也称信息管理。在计算机系统中存有大量的文件，如何有效地组织与管理它们，并为用户提供一个使用方便的接口是文件系统的一大任务。

1）树形文件结构

在操作系统中，通常以文件目录的方式来组织和管理系统中的所有文件，并把文件目录组织成一个树形结构，整个文件系统有一个根，然后在根上分枝，任何一个分枝上都可以再分枝，枝上也可以长出树叶。根和枝称为目录或文件夹。而叶子则是一个个的文件。实践证明，此种结构的文件系统效率比较高。例如，图 2-11 就是一个树形的目录结构，其中方框代表目录，圆形代表文件。

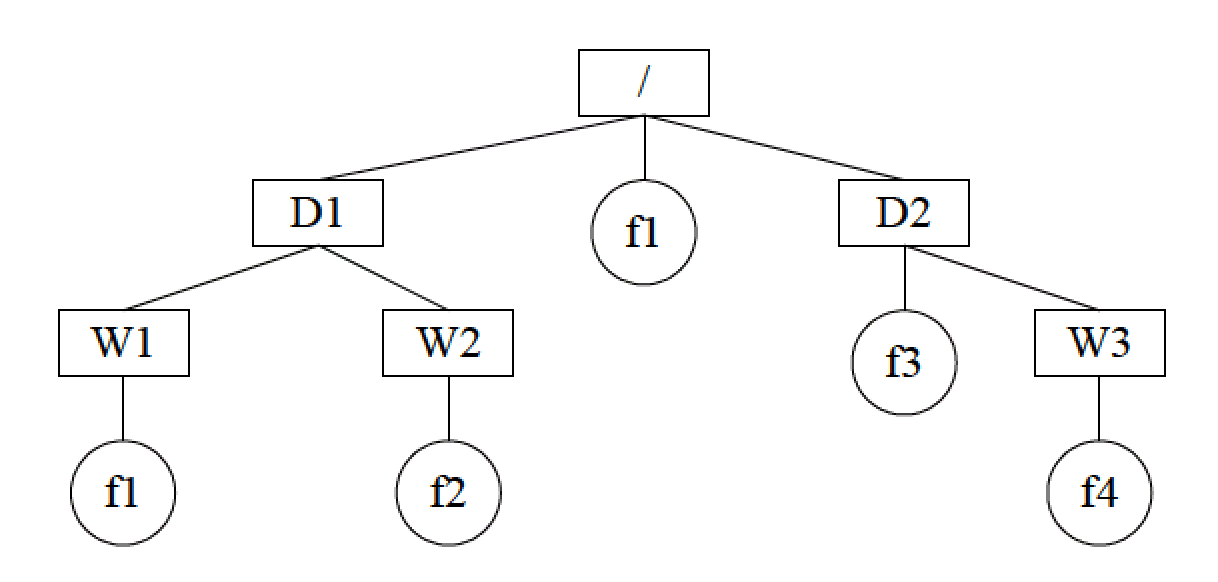


图 2-11　树形文件结构

在树形目录结构中，树的根节点为根目录，数据文件作为树叶，其他所有目录均作为树的节点。系统在建立每一个目录时，都会自动为它设定两个目录文件，一个是“.”，代表该目录自己，另一个是“..”，代表该目录的父目录，对于根目录，“.”和“..”都代表其自己。

从逻辑上讲，用户在登录到系统中之后，每时每刻都处在某个目录之中，此目录被称作工作目录或当前目录，工作目录是可以随时改变的。

对文件进行访问时，需要用到路径的概念。路径是指从树形目录中的某个目录层次

到某个文件的一条道路。在树形目录结构中，从根目录到任何数据文件之间，只有一条唯一的通路，从树根开始，把全部目录文件名与数据文件名依次用“/”连接起来，构成该数据文件的路径名，且每个数据文件的路径名是唯一的。这样，可以解决文件重名问题，不同路径下的同名文件不一定是相同的文件。例如，在图 2-11 中，根目录下的文件 f1 和/D1/W1 目录下的文件 f1 可能是相同的文件，也可能是不相同的文件。

用户在对文件进行访问时，要给出文件所在的路径。路径又分相对路径和绝对路径。绝对路径是指从根目录开始的路径，也称为完全路径；相对路径是从用户工作目录开始的路径。应该注意到，在树形目录结构中到某一确定文件的绝对路径和相对路径均只有一条。绝对路径是确定不变的，而相对路径则随着用户工作目录的变化而不断变化。

用户要访问一个文件时，可以通过路径名来引用。例如，在图 2-11 中，如果当前路径是 D1，则访问文件 f2 的绝对路径是/D1/W2/f2，相对路径是 W2/f2。如果当前路径是 W1，则访问文件 f2 的绝对路径仍然是/D1/W2/f2，但相对路径变为../W2/f2。

在 Windows 系统中，有两种格式的文件，分别是 FAT32（FAT16）文件和 NTFS 文件。NTFS 在使用中产生的磁盘碎片要比 FAT32 少，安全性也更高，而且支持单个文件的容量更大，超过了 4GB，特别适合现在的大容量存储。NTFS 可以支持的分区（如果采用动态磁盘则称为卷）大小可以达到 2TB。而 Windows 2000 中的 FAT32 支持分区的大小最大为 32GB。

2）管道

管道通信方式的中间介质是文件，通常称这种文件为管道文件。两个进程利用管道文件进行通信时，一个进程为写进程，另一个进程为读进程。写进程通过写端（发送端）往管道文件中写入信息；读进程通过读端（接收端）从管道文件中读取信息。两个进程协调不断地进行写、读，便会构成双方通过管道传递信息的流水线。

管道（命名管道）用缓冲区存储数据，普通文件用磁盘存储数据。另外，命名管道的重要作用是用于进程间的通信。在 UNIX 系统中，管道命令可以起到输出重定向的作用。例如：

```
$ ps > a.txt
$ sort a.txt > b.txt
```

其中“>”是输出重定向符号，把标准输出重定向到另一个文件，如果该文件已经存在，则覆盖。如果使用“>>”符号，则把标准输出追加到另一个文件的尾部。这两条命令的作用是，首先把进程列表输出到文件 a.txt 中（ps 的作用是显示当前正在运行的进程列表）。然后，再对文件 a.txt 进行排序，把排序的结果写入 b.txt 中。如果这两条命令接上管道，则如下：

```
$ ps | sort > b.txt
```

其中，中“|”是管道符号。这条命令的作用与前面两条命令的作用是相同的。

2.2.3　数据库系统基础

在数据库系统基础方面，主要考查数据库概念、数据库模型、数据库功能、关系代数、SQL 语言等。

1．基本概念

数据库是指长期存储在计算机中，有组织的、可共享的数据的集合。数据库管理技术的发展大致经历了人工管理、文件系统、数据库系统三个阶段，如表 2-4 所示。

表 2-4　数据库管理技术各发展阶段

	人 工 管 理	文 件 系 统	数据库系统
数据存储	不保存	数据相互独立和分离	数据结构化
数据共享	不共享	共享性不好	良好共享
数据冗余性	无	高	低
数据独立性	无	差	高
数据管理者	应用程序	应用程序	DBMS

从表 2-4 可以看出，数据库管理技术是在文件系统的基础上发展起来的。建立数据库系统的主要目标也就是减少数据冗余，提高数据独立性，集中检查数据完整性。数据库系统的设计目标是允许用户逻辑地处理数据，而不必涉及这些数据在计算机中是怎样存放的，在数据组织和用户应用之间提供某种程度的独立性。

支持数据库各种操作的软件系统叫做数据库管理系统（DataBase Management System，DBMS），DBMS 是一种负责数据库定义、建立、操作、管理和维护的软件系统，主要由存储管理器和查询处理器组成。其目的在于保证数据安全可靠，提高数据库应用的简明性和方便性。DBMS 的工作机理是把用户对数据的操作转化为对系统存储文件的操作，有效地实现数据库三级之间的转化。数据库管理系统的主要职能有：数据库的定义和建立、数据库的操作、数据库的控制、数据库的维护、故障恢复和数据通信。

广义来说，数据库系统包括数据库、硬件、软件（应用程序）和数据库管理员（DBA）四个部分。它将数据库体系结构的描述存放在数据字典中，所以数据库管理系统对数据库的操作都要通过数据字典来进行。

1）三级模式

数据库系统的三级模式为概念模式、外模式和内模式。

- 概念模式：概念模式（模式、逻辑模式）用以描述整个数据库中数据库的逻辑结构，描述现实世界中的实体及其性质与联系，定义记录、数据项、数据的完整性约束条件及记录之间的联系，是数据项值的框架。概念模式通常还包含有访问控制、保密定义、完整性检查等方面的内容，以及概念/物理之间的映射。概念模式是数据库中全体数据的逻辑结构和特征的描述，是所有用户的公共数据视图。一

个数据库只有一个概念模式。

- 外模式：外模式（子模式、用户模式）用以描述用户看到或使用的那部分数据的逻辑结构，用户根据外模式用数据操作语句或应用程序去操作数据库中的数据。外模式主要描述组成用户视图的各个记录的组成、相互关系、数据项的特征、数据的安全性和完整性约束条件。外模式是数据库用户（包括程序员和最终用户）能够看见和使用的局部数据的逻辑结构和特征的描述，是数据库用户的数据视图，是与某一应用有关的数据的逻辑表示。一个数据库可以有多个外模式。一个应用程序只能使用一个外模式。
- 内模式：内模式是整个数据库的最低层表示，不同于物理层，它假设外存是一个无限的线性地址空间。内模式定义的是存储记录的类型、存储域的表示、存储记录的物理顺序，指引元、索引和存储路径等数据的存储组织。内模式是数据物理结构和存储方式的描述，是数据在数据库内部的表示方式。一个数据库只有一个内模式。

2）二级独立性

数据库系统两级独立性是指物理独立性和逻辑独立性。三级模式之间通过两级映射（外模式/模式映射，模式/内模式映射）进行相互转换，使得数据库的三级形成一个统一的整体。

- 物理独立性：物理独立性是指用户的应用程序与存储在磁盘上的数据库中的数据是相互独立的。当数据的物理存储改变时，应用程序不需要改变。物理独立性存在于概念模式和内模式之间的映射转换，说明物理组织发生变化时应用程序的独立程度。
- 逻辑独立性：逻辑独立性是指用户的应用程序与数据库中的逻辑结构是相互独立的。当数据的逻辑结构改变时，应用程序不需要改变。逻辑独立性存在于外模式和概念模式之间的映射转换，说明概念模式发生变化时应用程序的独立程度。

值得注意的是，逻辑独立性比物理独立性更难实现。

2．数据模型的类型

数据模型主要有两大类，分别是概念数据模型（实体联系模型）和基本数据模型（结构数据模型）。

1）概念数据模型

概念数据模型是按照用户的观点来对数据和信息建模，主要用于数据库设计。概念模型主要用实体联系方法表示，所以也称 E-R 模型。

基本数据模型是按照计算机系统的观点对数据和信息建模，主要用于 DBMS 的实现。基本数据模型是数据库系统的核心和基础。基本数据模型通常由数据结构、数据操作和完整性约束三部分组成。其中数据结构是对系统静态特性的描述，数据操作是对系统动态特性的描述，完整性约束是一组完整性规则的集合。

2）基本数据模型

常用的基本数据模型有层次模型、网状模型、关系模型和面向对象模型。

层次模型用树形结构表示实体类型及实体间联系。层次模型的优点是记录之间的联

系通过指针来实现，查询效率较高。层次模型的缺点是只能表示 1:n 联系，虽然有多种辅助手段实现 m:n 联系，但较复杂，用户不易掌握。由于层次顺序的严格和复杂，使得数据的查询和更新操作很复杂，应用程序的编写也比较复杂。

网状模型用有向图表示实体类型及实体间联系。网状模型的优点是记录之间的联系通过指针实现，m:n 联系也容易实现，查询效率高。其缺点是编写应用程序比较复杂，网络管理员必须熟悉数据库的逻辑结构。

关系模型用表格结构表达实体集，用外键表示实体间联系，其优点有：

（1）建立在严格的数学概念基础上。

（2）概念单一（关系），结构简单、清晰，用户易懂易用。

（3）存取路径对用户透明，从而数据独立性、安全性好，简化数据库开发工作。

（4）关系模型的缺点主要是由于存取路径透明，查询效率往往不如非关系数据模型。

面向对象数据模型是一种可扩充的数据模型，它吸收了语义数据模型和知识表示模型的一些基本概念，同时又借鉴了面向对象程序设计语言和抽象数据类型的一些思想。面向对象模型中最基本的概念是对象（object）和类（class）。对象是现实世界中实体的模型化，与记录概念相仿，但远比记录复杂。每一个对象有一个唯一的标识符，把状态和行为封装在一起。其中，对象的状态是该对象属性值的集合，对象的行为是在对象状态上操作的方法集。共享同一属性集和方法集的所有对象构成一个类。

3．关系模型

关系模型是目前最重要的一种数据模型。关系数据库系统就是采用关系模型作为数据的组织方式。关系数据模型是以集合论中的关系概念为基础发展起来的数据模型，而关系运算是关系数据模型的理论基础。

在关系模型中，现实世界的实体以及实体间的各种联系均用关系来表示。用二维表格结构表达实体类型，外键表示实体间联系的模型称为关系模型。关系模型是建立在集合代数的基础上的。下面从集合论角度给出关系数据结构的形式化定义，并介绍关系模型及有关的基本概念。

（1）域：一组具有相同数据类型的值的集合。

（2）笛卡儿积：给定一组域 $D_1,D_2,\cdots,D_n$，其中可以有相同的域。$D_1,D_2,\cdots,D_n$ 的笛卡儿积为：

$$D_1\times D_2\times\cdots\times D_n=\{(d1,d2,\cdots,dn)|d_j\in D_j, j=1,2,\cdots,n\}$$

其中每一个元素（$d_1,d_2,\cdots,d_n$）叫做一个 n 元组（简称为元组）。元组中的每一个值 d_j 叫做一个分量。

（3）关系：$D_1\times D_2\times\cdots\times D_n$ 的子集叫做在域 $D_1,D_2,\cdots,D_n$ 上的关系，表示为：

$$R(D_1,D_2,\cdots,D_n)$$

这里 R 表示关系的名字，n 是关系的目或度。

关系中的每个元素是关系中的元组，通常用 t 表示。关系是笛卡儿积的子集，所以关系也是一个二维表，表的每行对应一个元组，表的每列对应一个域。由于域可以相同，

为了加以区分，必须为每列起一个名字，称为属性。

派生属性是指可以由其他属性经过运算得到的属性，因而派生属性会产生冗余，通常不存储。例如，如果某关系中有年龄、出生日期这两个属性，则年龄就是派生属性，因为可用出生年月计算出年龄的值。

多值属性（组合属性）是指可同时由多个值表示的属性。例如，包含关于员工信息的关系可能包含关于员工兴趣的数据。一个员工可能有多个兴趣，例如运动、电影、投资、烹调等，并且由于这些值的任何一个或所有这些值可能同时是某一个员工的兴趣。

关系的度是指关系中属性的个数，关系的势是指关系中元组的个数。关系中的不同属性可以在相同的域中取值，属性的个数与域的个数并不相同。

关系可以有三种类型：基本关系（通常又称为基本表或基表）、查询表和视图表。基本表是实际存在的表，它是实际存储数据的逻辑表示。查询表是查询结果对应的表。视图表是由基本表或其他视图表导出的表，是虚表，不对应实际存储的数据。

基本关系具有以下 6 条性质：

（1）列是同质的，即每一列中的分量是同一类型的数据，来自同一个域。

（2）不同的列可出自同一个域，称其中的每一列为一个属性，不同的属性要给予不同的属性名。

（3）列的顺序无所谓，即列的次序可以任意交换。

（4）任意两个元组不能完全相同。但在大多数实际关系数据库产品中，例如 Oracle 等，如果用户没有定义有关的约束条件，它们都允许关系表中存在两个完全相同的元组。

（5）行的顺序无所谓，即行的次序可以任意交换。

（6）分量必须取原子值，即每一个分量都必须是不可分的数据项。

关系的描述称为关系模式。一个关系模式应当是一个五元组。它可以形式化地表示为：$R(U,D,\mathrm{DOM},F)$。其中 R 为关系名，U 为组成该关系的属性名集合，D 为属性组 U 中属性所来自的域，DOM 为属性向域的映像集合，F 为属性间数据的依赖关系集合。关系模式通常可以简记为：$R(A1,A2,\cdots,An)$。其中 R 为关系名，$A1,A2,\cdots,An$ 为属性名。

关系实际上就是关系模式在某一时刻的状态或内容。也就是说，关系模式是型，关系是它的值。关系模式是静态的、稳定的，而关系是动态的、随时间不断变化的，因为关系操作在不断地更新着数据库中的数据。但在实际当中，常常把关系模式和关系统称为关系，读者可以从上下文中加以区别。

在关系模型中，实体及实体间的联系都是用关系来表示的。联系归结为三种类型：

（1）一对一联系（1:1）。设 A，B 为两个实体集。若 A 中的每个实体至多和 B 中的一个实体有联系，反过来，B 中的每个实体至多和 A 中的一个实体有联系，称 A 对 B 或 B 对 A 是 1:1 联系。注意，1:1 联系不一定都是一一对应的关系。可能存在着无对应。例如，一个班只有一个班主任，一个班主任不能同时在其他班再兼任班主任，由于老师紧缺，某个班的班主任也可能暂缺。

（2）一对多联系（1:n）。如果实体集 A 中的每个实体可以和 B 中的几个实体有联系，而 B 中的每个实体至多和 A 中的一个实体有联系，那么 A 对 B 属于 1:n 联系。例如，一个班级有多个学生，而一个学生只能编排在一个班级，班级与学生属于一对多的联系。

（3）多对多联系（m:n）。若实体集 A 中的每个实体可与和 B 中的多个实体有联系，反过来，B 中的每个实体也可以与 A 中的多个实体有联系，称 A 对 B 或 B 对 A 是 m:n 联系。例如，一个学生可以选修多门课程，一门课程由多个学生选修，学生和课程间存在多对多的联系。

4．集合运算

传统的集合运算是二目运算，包括并、交、差、广义笛卡儿积四种运算。

1）并

设关系 R 和 S 具有相同的关系模式，R 和 S 的并是由属于 R 或属于 S 的元组组成的集合，记为 $R\cup S$。形式定义如下：

$$R\cup S\equiv\{t\,|\,t\in R\vee t\in S\}$$

式中 t 是元组变量（下同）。显然，$R\cup S$=$S\cup R$。

2）差

关系 R 和 S 具有相同的关系模式，R 和 S 的差是由属于 R 但不属于 S 的元组组成的集合，记为 R–S。形式定义如下：

$$R-S\equiv\{t\,|\,t\in R\wedge t\notin S\}$$

3）交

关系 R 和 S 具有相同的关系模式，R 和 S 的交是由既属于 R 又属于 S 的元组组成的集合，记为 $R\cap S$。形式定义如下：

$$R\cap S\equiv\{t\,|\,t\in R\wedge t\in S\}$$

显然，$R\cap S$=R–（R–S），或者 $R\cap S$ = S–（S–R）。

4）笛卡儿积

设关系 R 和 S 元数分别为 r 和 s。R 和 S 的笛卡儿积是一个 r+s 元的元组集合，每个元组的前 r 个分量来自 R 的一个元组，后 s 个分量来自 S 的一个元组，记为 $R\times S$。形成定义如下：

$$R\times S\equiv\{t\,|\,t=<t_r,t_s>\wedge t_r\in R\wedge t_s\in S\}$$

若 R 有 m 个元组，S 有 n 个元组，则 $R\times S$ 有 $m\times n$ 个元组。

5）集合运算实例

例如，设关系 R 和 S 如表 2-5 所示。则 $R\cup S$ 与 $R\cap S$ 如表 2-6 所示，R–S 和 S–R 如表 2-7 所示，$R\times S$ 如表 2-8 所示。

表 2-5 关系 R 和 S

R 关系				*S* 关系		
A1	*A2*	*A3*		*A1*	*A2*	*A3*
a	b	c		a	b	a
b	a	d		b	a	d
c	d	d		c	d	d
d	f	g		d	s	c

表 2-6 R∪S 与 R∩S

R∪*S*				*R*∩*S*		
A1	*A2*	*A3*		*A1*	*A2*	*A3*
a	b	c		b	a	d
b	a	d		c	d	d
c	d	d				
d	f	g				
a	b	a				
d	s	c				

表 2-7 R–S 和 S–R

R–S				*S–R*		
A1	*A2*	*A3*		*A1*	*A2*	*A3*
a	b	c		a	b	a
d	f	g		d	s	c

表 2-8 R×S

A1	*A2*	*A3*	*A1*	*A2*	*A3*
a	b	c	a	b	a
b	a	d	a	b	a
c	d	d	a	b	a
d	f	g	a	b	a
a	b	c	b	a	d
b	a	d	b	a	d
c	d	d	b	a	d
d	f	g	b	a	d
a	b	c	c	d	d
b	a	d	c	d	d
c	d	D	c	d	d

续表

A1	A2	A3	A1	A2	A3
d	f	g	c	d	d
a	b	c	d	s	c
b	a	d	d	s	c
c	d	d	d	s	c
d	f	g	d	s	c

5．关系运算

在上节的集合运算基础上，关系数据库还有一些专门的运算，主要有投影、选择、连接、除法和外连接。它们是关系代数最基本的操作，也是一个完备的操作集。在关系代数中，由这五种基本代数操作经过有限次复合的式子称为关系代数运算表达式。表达式的运算结果仍是一个关系。我们可以用关系代数表达式表示各种数据查询和更新处理操作。

1）投影

投影操作从关系 R 中选择出若干属性列组成新的关系，该操作对关系进行垂直分割，消去某些列，并重新安排列的顺序，再删去重复元组。记为：

$$\pi_A(R) \equiv \{t[A] \mid t \in R\}$$

其中 A 为 R 的属性列。

2）选择

选择操作在关系 R 中选择满足给定条件的所有元组，记为：

$$\sigma_F(R) \equiv \{t \mid t \in R \wedge F(t) = \text{true}\}$$

其中 F 表示选择条件，是一个逻辑表达式（逻辑运算符+算术表达式 ）。选择运算是从行的角度进行的运算。

3）θ 连接

θ 连接从两个关系的笛卡儿积中选取属性间满足一定条件的元组，记为：

$$R \underset{A\theta B}{\triangleright\triangleleft} S \equiv \{t_r t_s \mid t_r \in R \wedge t_s \in S \wedge t_r[A]\theta t_s[B]\}$$

其中 A 和 B 分别为 R 和 S 上度数相等且可比的属性组。θ 为“=”的连接，称为等值连接，记为：

$$R \underset{A=B}{\triangleright\triangleleft} S \equiv \{t_r t_s \mid t_r \in R \wedge t_s \in S \wedge t_r[A] = t_s[B]\}$$

如果两个关系中进行比较的分量必须是相同的属性组，并且在结果中把重复的属性列去掉，则称为自然连接，记为：

$$R \triangleright\triangleleft S \equiv \{t_r t_s \mid t_r \in R \wedge t_s \in S \wedge t_r[A] = t_s[B]\}$$

4）关系运算实例

设两个关系模式 R 和 S 如表 2-9 所示，则 $\pi_{1,2}(R)$ 的结果如表 2-10 所示，$\sigma_{1>2}(R)$ 的

结果如表 2-11 所示，$R \bowtie S$ 的结果如表 2-12 所示。

表 2-9　关系 R 和 S

R 关系				*S* 关系		
*A*1	*A*2	*A*3		*A*1	*A*2	*A*3
a	b	c		a	z	a
b	a	d		b	a	h
c	d	d		c	d	d
d	f	g		d	s	c

表 2-10　对关系 R 求投影操作

*A*1	*A*2
a	b
b	a
c	d
d	f

表 2-11　对关系 R 求选择操作

*A*1	*A*2	*A*3
b	a	d

表 2-12　对关系 R 和 S 的自然连接

*A*1	*A*2	*A*3	*A*4
b	a	d	h
c	d	d	d

6．SQL 语言

SQL 是关系数据库的标准语言，对关系模型的发展和商用 DBMS 的研制起着重要的作用。SQL 语言是介于关系代数和元组演算之间的一种语言。

SQL-86 是第一个 SQL 标准，后续的有 SQL-89、SQL-92（SQL2）、SQL-99（SQL3）等。但作为考试而言，所考查的是一些基本的语法知识。

在 SQL 语言方面，主要考查定义查询基本表语句。

1）定义基本表

SQL 语言使用动词 CREATE 定义基本表，其具体语法格式如下：

```
CREATE TABLE <表名>
(<列名><数据类型>[列级完整性约束条件][,
<列名><数据类型>[列级完整性约束条件]][,
<表级完整性约束条件>]);
```

2）基本表查询

SQL 语言查询语句的基本格式如下：

```
SELECT [ALL|DISTINCT] <目标列表达式>[, <目标列表达式>]…
FROM <表或视图名>[, <表或视图名>]…
[WHERE <条件表达式>]
    [GROUP BY <列名 1> [HAVING <条件表达式>]]
    [ORDER BY <列名 2> [ASC|DESC]];
```

3）修改基本表

修改基本表的命令格式如下：

```
ALTER TABLE <表名>
[ADD <新列名><数据类型>[完整性约束]]
[DROP <完整性约束名>]
[MODIFY <列名><数据类型>];
```

例如，向 Student 表增加入学时间（Scome）列，其数据类型为日期型。SQL 命令如下：

```
ALTER TABLE Student Add Scome Date;
```

4）删除基本表

删除基本表的命令格式如下：

```
DROP TABLE <表名>
```

例如，要删除 Student 表的命令为：

```
DROP TABLE Student;
```

注意：基本表一旦删除，表中的数据、表上建立的索引和视图都将自动被删除。

5）插入数据

插入单个元组的命令格式为：

```
INSERT INTO <表名>[(<属性列 1>[,<属性列 2>]…] )
VALUES (<常量 1>[,<常量 2>]…)
```

例如，将一个新学生记录（95020，陈冬，男，IS，18）插入到 Student 表中。

```
INSERT INTO Student
VALUES ('95020', '陈冬', '男', 'IS',18);
```

如果省略了表名后面的属性列，则 VALUES 后面的数据顺序要和表定义时属性的顺序是完全一致的。如果某些属性可以取空值或者不按照定义时的顺序，则可以写为：

```
INSERT INTO Student (SName, SNo, Sage)
```

```
VALUES ('陈冬', '95020', 18);
```

插入成批数据或从一个表中导入数据到另一个表中的命令格式如下：

```
INSERT INTO <表名1> [(<属性列1>[,<属性列2>]…) ]
SELECT [(<属性列1>[,<属性列2>]…) ]
FROM <表名2>
```

这里要求两个属性列表要完全一致。

6）修改数据

修改数据的命令格式为：

```
UPDATE <表名>
SET <列名1>=<表达式1>[,<列名2>=<表达式2>]…
[WHERE <条件>]
```

例如，将学生 95001 的年龄改为 22 岁。

```
UPDATE Student
SET Sage=22
WHERE Sno='95001';
```

7）删除数据

删除表中数据的命令格式为：

```
DELETE FROM <表名>
[WHERE <条件>]
```

例如，删除学号为 95019 的学生记录为：

```
DELETE FROM Student
WHERE Sno='95019';
```

2.2.4 程序设计语言

程序设计语言用以书写计算机程序（指计算任务的处理对象和处理规则的描述），它包括语法、语义、语用三个方面。语法表示程序的结构或形式，即表示构成语言的各记号间的组合规则，但不涉及这些记号的特定含义，也不涉及使用者。语义表示程序的含义，即表示按照各种方法所表示的各个记号的特定含义，但不涉及使用者。语用表示程序与使用者的关系。

程序设计语言的基本成分有数据、运算、控制和传输。数据成分用以描述程序中所涉及到的数据；运算成分用以描述程序中所包含的运算；控制成分用以表达程序中的控制构造；传输成分用以表达程序中数据的传输。

1．编译设计基础

编译程序（编译器）的职能是把使用某种高级程序设计语言书写的程序翻译为等价的机器语言程序。一般来说，编译程序分为以下几个部分：词法分析、语法分析和语义分析、代码优化、代码生成和符号表管理。各部分之间的关系如图 2-12 所示。

2．解释系统基础

解释程序是一种语言处理程序，它实际是一台虚拟的机器，直接理解执行源程序或源程序的内部形式（中间代码）。因此，解释程序并不产生目标程序，这是它和编译程序的主要区别。图 2-13 显示了解释程序实现的三种可能情况。

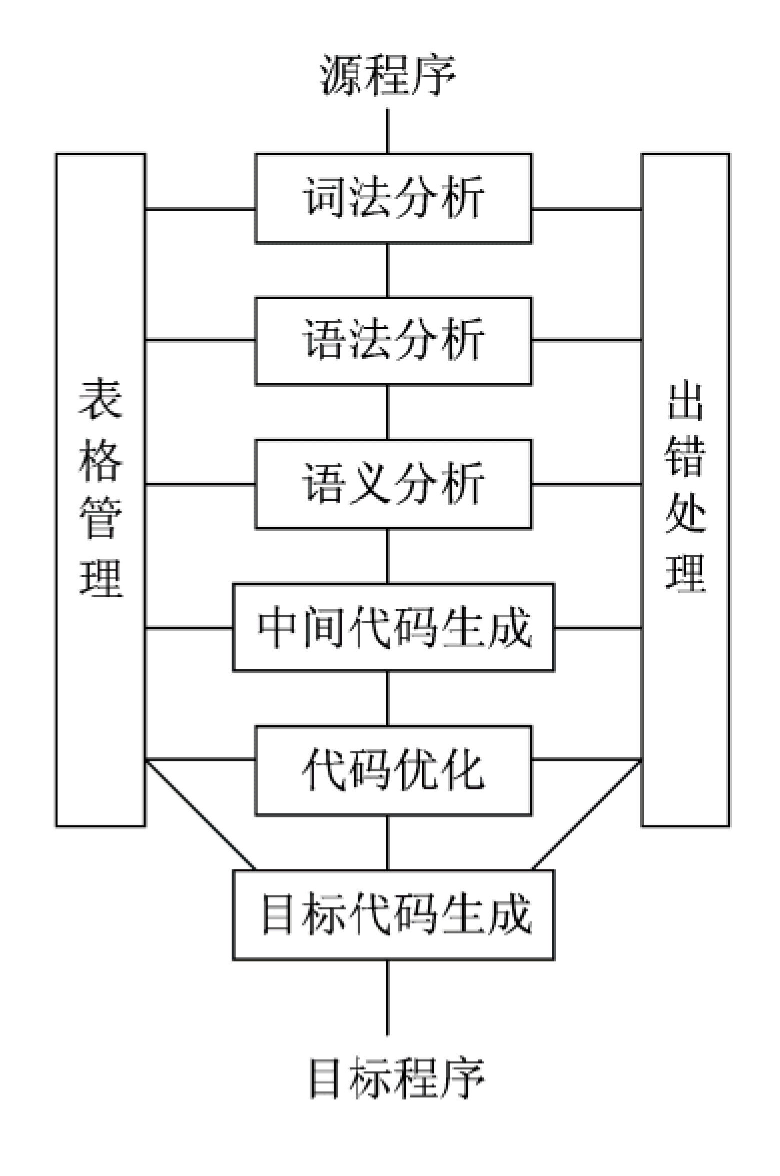


图 2-12　编译系统

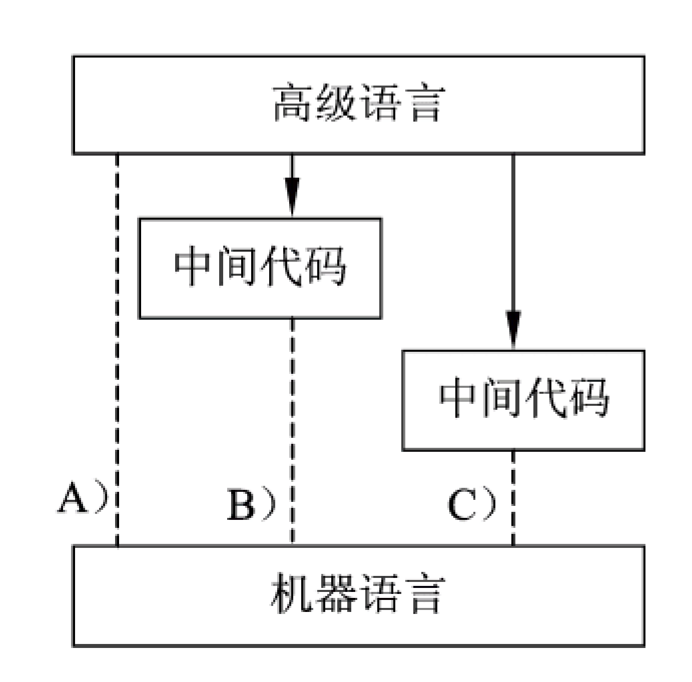


图 2-13　解释系统

在类型 A 的实现方案中，解释程序直接对源程序进行解释执行。这种解释程序对源程序进行逐字符的检查，然后执行程序指令表示的动作。例如，当解释程序扫描到字符串序列 GOTO Label，解释程序意识到 GOTO 命令代表无条件跳转至 Label 所标识的位置，于是就开始搜索源程序中标号 Label 后面紧跟冒号“：”的出现位置，然后跳转至该位置继续执行。这类系统在实现时需要反复扫描源程序，因此按类型 A 方案实现的解释程序效率很低，早期的解释性 Basic 语言就是采取该方案实现的。

在类型 B 的实现方案中，翻译程序先将源程序翻译成较贴近高级语言的高级中间代码，然后再扫描高级中间代码，对高级中间代码进行解释执行。所谓较贴近高级语言的高级中间代码，是指中间代码与高级语言的语句形式相像，两者存在着一一对应的关系。

类型 C 又是一种解释程序的实现方案。类型 C 的解释程序和类型 B 的解释程序不同点在于，类型 C 的解释程序首先将源程序转化成和机器代码十分接近的低级中间代码，然后再解释执行这种低级中间代码。一般说来，在这种实现方案下，高级语言的语句和

低级中间代码之间存在着 1:n 对应关系。例如微软的 C#语言，首先被编译成一种形式上较类似汇编语言的中间语言 IL 表示的代码，然后通过通用语言运行时（Common Language Runtime，CLR）解释执行 IL 程序。这类系统具有良好的可移植性。

3．常量与变量

常量是在程序运行过程中值不修改的数据。常量具有名字，便于望文生义，也可以方便的引用，需要时仅修改常量定义处，因此可以提高程序的可读性以及可维护性。

变量是在程序运行过程中可以修改的数据。变量也具有名字，变量可以分为局部变量和全局变量。

局部变量也称为内部变量。局部变量是在函数内作定义说明的。其作用域仅限于函数内，离开该函数后再使用这种变量是非法的。

全局变量也称为外部变量，它是在函数外部定义的变量。它不属于哪一个函数，它属于一个源程序文件。其作用域是整个源程序。在函数中使用全局变量，一般应作全局变量说明。只有在函数内经过说明的全局变量才能使用。

在程序中，函数中定义的变量是局部变量，在函数之外定义的变量为外部变量，外部变量是全局变量。二者的有效范围不一样，前者只在本函数范围内有效，后者的有效范围从定义该全局变量的位置开始到本源文件结束。

作为一种好的习惯，变量在使用前必须设置初始值。否则，如果程序中使用的变量未设置初始值，则运行结果可能会出错。

一般变量处于内存中，如果某一变量被频繁使用，则可以将其定义为寄存器变量，将变量放在寄存器中，由于运算器访问寄存器的速度远远大于访问内存的速度，可以节省不少时间。

4．控制结构

表达式的顺序控制是把操作数和操作符看做基本单位，研究操作符的计算顺序。而语句间的顺序控制是把程序语句作为基本单位，研究语句执行的顺序。程序语言对语句的执行都遵循一条隐含规则，这就是在没有其他顺序控制结构规定的情况下，按照语句在程序中的物理位置执行程序，也就是顺序执行。改变这种语句执行次序的方法是使用程序顺序控制结构，这些控制结构有跳转结构、选择结构（分支结构）和循环结构（重复结构）。其中，跳转结构是不主张使用的。因此，程序的基本控制结构主要有顺序结构、选择结构和循环结构

1）跳转结构

跳转结构就是令程序控制无条件地从当前语句转向给定的语句执行的控制结构，跳转语句的执行非常有效，它反映了计算机本身硬件的转移指令，如 x86 指令中的 jmp 指令。通常的跳转语句都有如下形式：goto <标号>，Fortran 和 C 等语言都提供了 goto 语句。当程序控制遇到 goto 语句时，会转移到标号所指出的相应语句继续执行。

虽然 goto 语句的使用十分简单和高效，但是大量的使用会令程序控制逻辑混乱，程

序变得难以理解和维护。人们已经证明可以使用顺序结构、选择结构和循环结构组成任何程序，而抛弃掉“有害的”goto 语句。目前比较一致的观点是程序员必须谨慎地使用 goto 语句，使用时必须考虑是否可以用更好的结构来代替。

2）选择结构

选择结构是对给定条件进行判断，然后根据结果执行不同的语句或语句块的结构。最典型的选择结构的形式如下：

```
If <expr> then
        <statements1>
    Else
        <statements2>
Endif
```

意味着如果 expr 条件为真则执行 statements1 语句块，否则执行 statements2 语句块。在某些复杂的情况下，需要对多个条件进行判断，则 if-then-else 语句会进一步复杂，演化为 if-then-elseif-then-else 等。

在两个分支的选择结构基础上，多数语言也会提供多分支的选择结构，它在许多情况下可以改善程序的可读性。典型的多分支选择结构如下：

```
Switch (<expr>)
Case of result1:
<statements1>
Case of result2:
<statements2>
…
Default:
<default_statements>
Endswitch
```

虽然 case 控制结构的功能可以由 if-then-else 结构来模拟，但是 case 控制结构能提供更清晰的计算过程的反映。

C/C++的情况比较特别，在 case 结构中使用 break 语句表示跳出结构的控制，如果在其中一个 case 中没有使用 break 语句，则控制会顺序执行至下一个 case 中的语句。这个特点在为程序员带来方便的同时，也为程序员带来了麻烦。程序员疏忽漏掉的 break 语句会导致程序有意想不到的执行结构。因此在 C#中，语言再不允许这种 case 的“贯穿”，而强制程序员使用 goto 语句跳转至相应的 case 标号，以保证程序员清楚知道程序控制的行为。

3）循环结构

循环结构是根据条件重复执行指定语句的控制结构。循环结构是由循环头和循环体

组成的。循环头就是循环的条件，用以控制循环的次数，循环体则是提供动作的语句。典型的循环头结构有以下几种：

（1）计数器循环。

这种结构需要说明一个循环计数器，并且在头部中说明计数器的初值、终值和增量。典型的计数器循环的结构是 Pascal 的计数器循环：

```
for i:=0 to 30 step 2 Do <body>
```

该循环的头部说明了计数器为 i，其初值为 0，终值为 30，增量为 2，循环的执行次数为 16 次。

（2）条件循环。

条件循环是指在给出的条件表达式成立时重复执行循环体的循环结构，它的头部中说明了该条件表达式。这种循环期望在循环体执行的时候会改变条件测试表达式中的某个变量的值，否则循环将永不终止。典型的条件循环的结构有两种，一是 while <expr> do <body>，另一种是 repeat <body> until <expr>（do <body> while <expr>）。前者是先测试条件，然后执行循环体，循环体执行 0 次或 0 次以上。而后者是先执行循环体，再测试条件，循环体执行 1 次或 1 次以上。

例如，若循环体执行的次数为 m，则在 do-while 循环中，循环条件的执行次数为 m，在 while-do 循环中，判断循环条件的次数为 $m+1$。这是因为 do-while 循环是先执行循环体再判断循环条件，也就是至少会执行一次循环体，循环条件的判断次数与循环体的执行次数是相等的；while-do 循环是先判断循环条件再执行循环体，也就是循环体可能一次都不执行，即循环条件的判断次数要比循环体的执行次数多 1。

（3）基于数据的循环。

基于数据的循环的循环次数是由数据格式决定的。例如 C#中的 foreach 结构：

```
foreach (object o in <collection>) {…}
```

对于每一次循环，变量 o 都会取得数据集中的下一个值，数据集元素的个数决定了循环的次数。

（4）不定循环。

如果循环结束条件过于复杂，不容易在头部表示，通常会使用在循环头部没有显示终止测试的无限循环，然后在循环体中通过条件判断退出循环。C/C++中有两种典型的不定循环结构，一是 for (;;) <statements>，另外是 while(1)<statements>。

2.2.5 面向对象方法

在面向对象方法方面，主要考查面向对象的基本概念、数据隐藏、UML、构件等。

1. 基本概念

面向对象方法包括面向对象的分析、面向对象的设计和面向对象的程序设计。我们

首先介绍面向对象方法的一些基本概念。

1）对象

在计算机系统中，对象是指一组属性以及这组属性上的专用操作的封装体。属性可以是一些数据，也可以是另一个对象。每个对象都有它自己的属性值，表示该对象的状态，用户只能看见对象封装界面上的信息，对象的内部实现对用户是隐蔽的。封装的目的是使对象的使用者和生产者分离，使对象的定义和实现分开。一个对象通常由三部分组成，分别是对象名、属性和操作（方法）。

2）类

类是一组具有相同属性和相同操作的对象的集合。一个类中的每个对象都是这个类的一个实例（instance）。在分析和设计时，我们通常把注意力集中在类上，而不是具体的对象上。通常把一个类和这个类的所有对象称为类及对象或对象类。

一个类通常由三部分组成，分别是类名、属性和操作（方法）。每个类一般都有实例，没有实例的类是抽象类。抽象类不能被实例化，也就是不能用 new 关键字去产生对象，抽象方法只需声明，而不需实现。抽象类的子类必须覆盖所有的抽象方法后才能被实例化，否则这个子类还是个抽象类。

是否建立了丰富的类库是衡量一个面向对象程序设计语言成熟与否的重要标志之一。

3）继承

继承是在某个类的层次关联中不同的类共享属性和操作的一种机制。一个父类可以有多个子类，这些子类都是父类的特例。父类描述了这些子类的公共属性和操作，子类还可以定义它自己的属性和操作。一个子类只有唯一的父类，这种继承称为单一继承。一个子类有多个父类，可以从多个父类中继承特性，这种继承称为多重继承。对于两个类 A 和 B，如果 A 类是 B 类的子类，则说 B 类是 A 类的泛化。继承是面向对象方法区别于其他方法的一个核心思想。

4）封装

面向对象系统中的封装单位是对象，对象之间只能通过接口进行信息交流，外部不能对对象中的数据随意地进行访问，这就造成了对象内部数据结构的不可访问性，也使得数据被隐藏在对象中。封装的优点体现在好的封装能减少耦合，类的内部的实现可以自由改变和一个类有更清楚的接口三个方面。

5）消息

消息是对象间通信的手段、一个对象通过向另一对象发送消息来请求其服务。一个消息通常包括接收对象名、调用的操作名和适当的参数（如有必要）。消息只告诉接收对象需要完成什么操作，但并不能指示接收者怎样完成操作。消息完全由接收者解释，接收者独立决定采用什么方法来完成所需的操作。

6）多态性

多态性是指同一个操作作用于不同的对象可以有不同的解释，产生不同的执行结果。与多态性密切相关的一个概念就是动态绑定。传统的程序设计语言把过程调用与目标代码的连接放在程序运行前进行，称为静态绑定。而动态绑定则是把这种连接推迟到运行时才进行。在运行过程中，当一个对象发送消息请求服务时，要根据接收对象的具体情况将请求的操作与实现的方法连接，即动态绑定。

7）构件

构件（组件）是一个功能相对独立的具有可重用价值的软件单元。在面向对象方法中，一个构件由一组对象构成，包含了一些协作的类的集合，它们共同工作来提供一种系统功能。

可重用性是指系统和（或）其组成部分能在其他系统中重复使用的程度。软件开发的全生命周期都有可重用的价值，包括项目的组织、软件需求、设计、文档、实现、测试方法和测试用例，都是可以被重复利用和借鉴的有效资源。可重用性体现在软件的各个层次，通用的、可复用性高的软件模块往往已经由操作系统或开发工具提供，如通用库（函数库）、标准组件和标准模板库等，并不需要程序员重新开发。

2．统一建模语言

UML 是一种定义良好、易于表达、功能强大且普遍适用的建模语言。它溶入了软件工程领域的新思想、新方法和新技术。它的作用域不限于支持面向对象的分析与设计，还支持从需求分析开始的软件开发的全过程。

在这个知识点，要求我们掌握 UML 的图形、类之间的关系、用例之间的关系。

1）UML 的图形

UML 2.0 包括 14 种图，分别列举如下：

- 类图（Class Diagram）：展现了一组类、接口、协作和它们之间的关系。在面向对象系统的建模中所建立的最常见的图就是类图。类图给出系统的静态设计视图。包含主动类的类图给出系统的静态进程视图。
- 对象图（Object Diagram）：展现了一组对象以及它们之间的关系。对象图描述了在类图中所建立的事物的实例的静态快照。和类图一样，这些图给出系统的静态设计视图或静态进程视图，但它们是从真实案例或原型案例的角度建立的。
- 构件图（Component Diagram）：展现了一个封装的类和它的接口、端口以及由内嵌的构件和连接件构成的内部结构。构件图用于表示系统的静态设计实现视图。对于由小的部件构建大的系统来说，构件图是很重要的。构件图是类图的变体。
- 组合结构图（Composite Structure Diagram）：它可以描绘结构化类（例如构件或类）的内部结构，包括结构化类与系统其余部分的交互点。它显示联合执行包含结构化类的行为的部件配置。组合结构图用于画出结构化类的内部内容。
- 用例图（Use Case Diagram）：展现一组用例、参与者（一种特殊的类）及它们

之间的关系。用例图给出系统的静态用例视图。这些图在对系统的行为进行组织和建模上是非常重要的。

- 顺序图和通信图：两者都是交互图。交互图（Interaction Diagram）展现了一种交互，它由一组对象或角色以及它们之间可能发送的消息构成。交互图专注于系统的动态视图。顺序图（Sequence Diagram）是强调消息的时间次序的交互图；通信图（Communication Diagram）也是一种交互图，它强调收发消息的对象或角色的结构组织。顺序图和通信图表达了类似的基本概念，但每种图所强调概念的不同视图，顺序图强调的是时序，通信图则强调消息流经的数据结构。
- 状态图（State Diagram）：展现一个状态机，它由状态、转移、事件和活动组成。状态图展现了对象的动态视图。它对于接口、类或协作的行为建模尤为重要，而且它强调事件导致的对象行为，这非常有助于对反应式系统建模。
- 活动图（Activity Diagram）：将进程或其他计算的结构展示为计算内部一步步的控制流和数据流。活动图专注于系统的动态视图。它对于系统的功能建模特别重要，并强调对象间的控制流程。
- 部署图（Deployment Diagram）：展现了对运行时的处理节点以及在其中生存的构件的配置。部署图给出了体系结构的静态部署视图。通常一个节点包含一个或多个制品。
- 制品图（Artifact Diagram）：展现计算机中一个系统的物理结构。制品包括文件、数据库和类似的物理比特集合。制品图通常与部署图一起使用。制品也展现了它们实现的类和构件。
- 包图（Package Diagram）：展现由模型本身分解而成的组织单元以及它们的依赖关系。
- 定时图（Timing Diagram）：是一种交互图，它展现了消息跨越不同对象或角色的实际时间，而不仅仅是关心消息的相对顺序。
- 交互概览图（Interaction Overview Diagram）：是活动图和顺序图的混合物。

2）用例之间的关系

两个用例之间的关系可以概括为两种情况。一种是用于重用的包含关系，用构造型 include 或 use 表示；另一种是用于分离出不同行为的扩展，用构造型 extend 表示。

- 包含关系：当可以从两个或两个以上的原始用例中提取公共行为，或者发现能够使用一个构件来实现某一个用例的部分功能很重要时，我们应该使用包含关系来表示它们。
- 扩展关系：如果一个用例明显地混合了两种或两种以上的不同场景，即根据情况可能发生多种事情。我们可以断定将这个用例分为一个主用例和一个或多个辅用例描述可能更加清晰。

另外，用例之间还存在一种泛化关系。用例可以被特别列举为一个或多个子用例，这被称做用例泛化。当父用例能够被使用时，任何子用例也可以被使用。例如，我们购

买飞机票，即可以是电话订票，也可以是网上订票，则订票用例就是电话订票和网上订票的抽象。

3）类之间的关系

- 关联关系：描述了给定类的单独对象之间语义上的连接。关联提供了不同类之间的对象可以相互作用的连接。其余的关系涉及到类元自身的描述，而不是它们的实例。用“ ——— ”表示。
- 依赖关系：有两个元素 X，Y，如果修改元素 X 的定义可能会引起对另一个元素 Y 的定义的修改，则称元素 Y 依赖于元素 X。在 UML 中，使用带箭头的虚线“------►”表示依赖关系。

在类中，依赖由各种原因引起，例如，一个类向另一个类发送消息，一个类是另一个类的数据成员，一个类是另一个类的某个操作参数。如果一个类的接口改变，它发出的任何消息可能不再合法。

- 泛化关系：泛化关系描述了一般事物与该事物中的特殊种类之间的关系，也就是父类与子类之间的关系。继承关系是泛化关系的反关系，也就是说子类是从父类继承的，而父类则是子类的泛化。在 UML 中，使用带空心箭头的实线“———▷”表示泛化关系，箭头指向父类。
- 聚合关系：聚合是一种特殊形式的关联，它是传递和反对称的。聚合表示类之间的关系是整体与部分的关系。例如一辆轿车包含四个车轮、一个方向盘、一个发动机和一个底盘，就是聚合的一个例子。在 UML 中，使用一个带空心菱形的实线“———◇”表示聚合关系，空心菱形指向的是代表“整体”的类。
- 组合关系：如果聚合关系中的表示“部分”的类的存在与否，与表示“整体”的类有着紧密的关系，例如“公司”与“部门”之间的关系，那么就应该使用“组合”关系来表示这种关系。在 UML 中，使用带有实心菱形的实线“———◆”表示组合关系。

实现关系将说明和实现联系起来。接口是对行为而非实现的说明，而类之中则包含了实现的结构。一个或多个类可以实现一个接口，而每个类分别实现接口中的操作。用“ - - - - - ▷”表示。

流关系将一个对象的两个版本以连续的方式连接起来。它表示一个对象的值、状态和位置的转换。流关系可以将类元角色在一次相互作用中连接起来。流的种类包括变成（同一个对象的不同版本）和拷贝（从现有对象创造出一个新的对象）两种。用“ - - - - - >”表示。

2.3 例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 12 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

CPU 执行算术运算或者逻辑运算时，算术逻辑运算部件（ALU）将计算结果保存在__（1）__中。

（1）A. 累加器 AC　　B. 程序计数器 PC
C. 指令寄存器 IR　　D. 地址寄存器 AR

例题 1 分析

累加寄存器 AC 通常简称为累加器。它的功能是：当运算器的算术/逻辑单元（ALU）执行全部算术和逻辑运算时，为 ALU 提供一个工作区。例如，在执行一个加法前，先将一个操作数暂时存放在 AC 中，再从存放中取出另一个操作数，然后同 AC 的内容相加，所得结果送回 AC 中，而 AC 中原有的内容随即被破坏。顾名思义，累加寄存器用来暂时存放 ALU 运算的结果信息。显然，运算器中至少要有一个累加器寄存器。

例题 1 答案

（1）A

例题 2

若指令系统中设置了专用 I/O 操作指令，则 I/O 接口__（2）__。

（2）A. 与内存单元必须统一编址
B. 可以独立编址
C. 必须采用 DMA 方式与内存交换数据
D. 必须采用中断方式与内存交换数据

例题 2 分析

在计算机系统中，凡需要进行读写操作的部件都存在编址的问题。存储器的每个单元均有自己的地址，对于 I/O 接口，则需要对接口中的每个端口进行编址。通常采取两种编址方法：一种是独立编址，另一种是统一编址。

统一编址又称“存储器映射方式”。在这种编址方式下，I/O 端口地址置于存储器空间中，在整个存储空间中划出一部分空间给外设端口，端口和存储单元统一编址。其优点是无需专门的 I/O 指令，对端口操作的指令类型多，从而简化了指令系统的设计。缺点是端口占用存储器的地址空间，使存储器容量更加紧张，同时端口指令的长度增加，执行时间较长，端口地址译码器较复杂。

独立编址又称“I/O 映射方式”。这种方式的端口单独编址构成一个 I/O 空间，不占用存储器地址空间。其优点是端口所需的地址线较少，地址译码器较简单，采用专用的 I/O 指令，端口操作指令执行时间少，指令长度短。缺点是输入输出指令类别少，一般只能进行传送操作。

例题 2 答案

（2）B

例题 3

计算机的用途不同，对其部件的性能指标要求也有所不同。以科学计算为主的计算机，对__（3）__要求较高，所以应该重点考虑__（4）__。

（3）A. 外存储器的读写速度　　B. 主机的运算速度
C. I/O 设备的速度　　D. 显示分辨率

（4）A. CPU 的主频和字长，以及内存容量
B. 硬盘读写速度和字长
C. CPU 的主频和显示分辨率
D. 硬盘读写速度和显示分辨率

例题 3 分析

对于不同用途的计算机，其对不同部件的性能指标要求有所不同。例如：对于用作科学计算为主的计算机，其对主机的运算速度要求很高；对于用作大型数据库处理为主的计算机，其对主机的内存容量、存取速度和外存储器的读写速度要求较高；对于用作网络传输的计算机，则要求有很高的 I/O 速度，因此应当有高速的 I/O 总线和相应的 I/O 接口。

计算机的运算速度是指计算机每秒钟执行的指令数。单位为每秒百万条指令（简称 MIPS）或者每秒百万条浮点指令（简称 MFPOPS）。它们都是用基准程序来测试的。影响运算速度的有如下几个主要因素：

（1）CPU 的主频：指计算机的时钟频率。它在很大程度上决定了计算机的运算速度。

（2）字长：CPU 进行运算和数据处理的最基本、最有效的信息位长度。

（3）指令系统的合理性：每种机器都设计了一套指令，一般均有数十条到上百条，例如：加、浮点加、逻辑与、跳转等等，组成了指令系统。

例题 3 答案

（3）A　（4）C

例题 4

微处理器中的 ALU 可执行算术运算和__（5）__操作。

（5）A. 浮点　　B. 定点　　C. 逻辑　　D. 控制

例题 4 分析

算术逻辑单元（Arithmetic-Logic Unit，ALU）是中央处理器（CPU）的执行单元，是所有中央处理器的核心组成部分，算术逻辑单元主要功能是专门执行算术和逻辑运算的数字运算，如加减乘（不包括整数除法）。绝大部分计算机指令都是由 ALU 执行的。ALU 从寄存器中取出数据，数据经过处理将运算结果存入 ALU 输出寄存器中。其他部件负责在寄存器与内存间传送数据。控制单元控制着 ALU，通过控制电路来告诉 ALU 该执行什么操作。

大部分 ALU 都可以完成以下运算：

（1）整数算术运算（加、减，有时还包括乘和除，不过成本较高）。

（2）位逻辑运算（与、或、非、异或）。

（3）移位运算（将一个字向左或向右移位或浮动特定位，而无符号延伸），移位可被认为是乘以 2 或除以 2。

例题 4 答案

（5）C

例题 5

CD-ROM 盘中的信息存储在__（6）__中。

（6）A. 内外圈磁道　　B. 螺旋形光道
　　C. 内外圈光道　　D. 螺旋形磁道

例题 5 分析

CD-ROM 光盘由碳酸脂做成，中心带有直径 15mm 的孔洞。在盘基上浇铸了一个螺旋状的物理光道，从光盘的内部一直螺旋到最外圈，光道内部排列着一个个蚀刻的“凹陷”，由这些“凹坑”和“平地”构成了存储的数据信息。由于读光盘的激光会穿过塑料层，因此需要在其上面覆盖一层金属反射层（通常为铝合金）使它可以反射光，然后再在铝合金层上覆盖一层丙烯酸的保护层。

例题 5 答案

（6）C

例题 6

__（7）__不属于程序语言翻译软件。

（7）A. 编译程序　　B. 解释程序　　C. 汇编程序　　D. 编辑程序

例题 6 分析

- 解释程序：所谓解释程序是高级语言翻译程序的一种，它将源语言（如 BASIC）书写的源程序作为输入，解释一句后就提交计算机执行一句，并不形成目标程序。就像外语翻译中的“口译”一样，说一句翻一句，不产生全文的翻译文本。这种工作方式非常适合于人通过终端设备与计算机会话，如在终端上打一条命令或语句，解释程序就立即将此语句解释成一条或几条指令并提交硬件立即执行且将执行结果反映到终端，从终端把命令打入后，就能立即得到计算结果。这的确是很方便的，很适合于一些小型机的计算问题。但解释程序执行速度很慢，例如源程序中出现循环，则解释程序也重复地解释并提交执行这一组语句，这就造成很大浪费。ASP、PHP、BASIC 等都是解释程序。
- 编译程序：这是一类很重要的语言处理程序，它把高级语言（如 FORTRAN、COBOL、Pascal、C 等）源程序作为输入，进行翻译转换，产生出机器语言的目标程序，然后再让计算机去执行这个目标程序，得到计算结果。编译程序工作时，先分析，后综合，从而得到目标程序。所谓分析，是指词法分析和语法分析；所

谓综合是指代码优化，存储分配和代码生成。为了完成这些分析综合任务，编译程序采用对源程序进行多次虽然编译过程本身较为复杂，但一旦形成目标文件，以后可多次使用。相反，对于小型题目或计算简单不太费机时的题目，则多选用解释型的会话式高级语言，如 BASIC，这样可以大大缩短编程及调试的时间。

- 汇编程序：汇编型编译程序用来将汇编语言编写的程序，按照一一对应的关系，转换成用机器语言表示的程序。使用汇编语言编写的程序，机器不能直接识别，要由一种程序将汇编语言翻译成机器语言，这种起翻译作用的程序叫汇编程序，汇编程序是系统软件中语言处理系统软件。汇编语言把汇编程序翻译成机器语言的过程称为汇编。

汇编语言比机器语言易于读写、调试和修改，同时具有机器语言全部优点。但在编写复杂程序时，相对高级语言代码量较大，而且汇编语言依赖于具体的处理器体系结构，不能通用，因此不能直接在不同处理器体系结构之间移植。

例题 6 答案

（7）D

例题 7

若程序中定义了局部变量与全局变量，则__（8）__。

（8）A. 在函数内只能访问局部变量，而不能访问全局变量

B. 局部变量与全局变量的名字不得相同

C. 若一个函数被多次调用，则其定义的局部变量必定分配同一个存储单元

D. 函数中定义的局部变量与全局变量同名时，在函数内引用的是局部变量

例题 7 分析

本题主要考查局部变量与全局变量的概念，具体见本章 2.2.4 节程序设计语言中的常量与变量。

例题 7 答案

（8）D

例题 8

给定工程项目 PROJ 和职工 EMP 实体集，若一个职工可以参加多个项目，一个项目可以由多个职工参加，那么，PROJ 和 EMP 之间应是一个__（9）__的联系。

（9）A．1:1　　B．n:1　　C．1:n　　D．m:n

例题 8 分析

- 多对多联系：如果实体集 E1 中每个实体可以与实体集 E2 中任意个（零个或多个）实体有联系，反之亦然，那么称 E1 和 E2 的联系是“多对多联系”，记为 M:N。
- 一对一联系：如果实体集 E1 中每个实体至多和实体集 E2 中的一个实体有联系，反之亦然，那么实体集 E1 和 E2 的联系称为“一对一联系”，记为 1:1。
- 一对多联系：如果实体集 E1 中每个实体可以与实体集 E2 中任意个（零个或多个）

实体间有联系，而 E2 中每个实体至多和 E1 中一个实体有联系，那么称 E1 对 E2 的联系是“一对多联系”，记为 1:N。

例题 8 答案

（9）D

例题 9

线性表采用顺序存储结构，若表长为 m，且在任何一个合法插入位置上进行插入操作的概率相同，则插入一个元素平均移动__（10）__个元素。

（10）A. m–1　　B. m/2　　C. m/2+1　　D. m

例题 9 分析

本题考查数据结构与算法的线性插入算法，是常考的知识点。

线性表长 m，因此位置有 m+1 个，分别为 1，2，…，m，m+1：

在第 1 个位置插入，需要移动 m 个元素；

在第 2 个位置插入，需要移动 m–1 个元素；

……

在第 m 个位置插入，需要移动 1 个元素；

在第 m+1 个位置插入（也就是表尾），需要移动 0 个元素；

因此平均移动的为（m+0)/2=m/2。

例题 9 答案

（10）D

例题 10

学生关系模式为 S（Sno, Sname, SD, Sage），其中：Sno 表示学生学号，Sname 表示学生姓名，SD 表示学生所在系，Sage 表示学生年龄。试将下面的 SQL 语句空缺部分补充完整，使其可以查询计算机系学生的学号、姓名和年龄。

```
SELECT Sno,Sname,SD,Sage
FROM S
WHERE __(11)__;
```

（11）A. SD=计算机　　B. SD='计算机'

C. 'SD'=计算机　　D. 'SD=计算机'

例题 10 分析

本题考查的是考生对 SELECT 语句语法的掌握情况，属于比较简单、基础的方面。SELECT 语句是 SQL 语言中核心的数据查询语句，其语法为：

```
SELECT [ALL|DISINCT] <目标列表达式>[，<目标列表达式>]…
FROM <表或视图名>[，<表或视图名>]…
[WHERE <条件表达式>]
```

```
[GROUP BY <列名 1> [HAVING <条件表达式>]]
[ORDER BY <列名 2> [ASC|DESC]];
```

在本题中，WHERE 子句中空出来的部分，显然是要填入“<条件表达式>”，而题目中要求的是查询“计算机系学生”，而表示学生所在系的字段是 SD，因此应该是 SD=‘计算机’。要注意的是匹配的内容是字符串，要用单引号括起来。因此正确的答案是 B。

例题 10 答案

（11）B

例题 11

在软件开发中使用函数库可＿（12）＿。

（12）A. 提高软件的执行速度　　B. 降低系统负载

C. 提高软件各部分之间的耦合度　　D. 提高软件的可重用性

例题 11 分析

软件重用可分为两个层次，一个层次是设计上的重用，另外一个层次是代码级的重用，而代码级的重用上又可分细分为两层，一个是基于源代码的重用，另外一个是基于组件的重用。不同的平台对于重用的观点上是不一样的，COM 和.NET 平台更多地是强调组件级的重用，而 STL 更多地是强调源码级的重用。函数是实现代码重用性的核心，通常将函数组织到函数库中，可以在以后类似的应用程序中重复使用。

例题 11 答案

（12）D

例题 12

若内存按字节编址，用存储容量为 8K×8 比特的存储器芯片构成地址编号 7000H 至 EFFFH 的内存空间，则至少需要＿（13）＿片。

（13）A. 4　　B. 6　　C. 8　　D. 10

例题 12 分析

这是一道经典的老题了，希赛教育的系列书中都提到该题目的解答方式。这类题，先求内存的容量，本题地址容量为 EFFFH–7000H＋1=8000H=2^{15}=32K，而内存是按字节编址，因此内存的存储容量为 32K×8 比特。又已知构成存储器芯片的容量为 8K×8，因此需要（32K/8K）×（8/8）=4 片该类型的存储器芯片。

例题 12 答案

（13）A

第 3 章　计算机网络基础

计算机网络源于计算机与通信技术的结合，始于 20 世纪 50 年代，在近 20 年得到了迅猛发展。目前计算机网络已广泛应用于各个领域，大型互联网络 Internet 已经成为全球信息基础设施之一。网络在计算机发展史中的作用和影响是如此重要，以至于有人称：网络就是计算机！

根据考试大纲的要求，本章需要考生掌握的内容主要有三大板块：数据通信基础知识、计算机网络基础知识和局域网技术基础。

3.1　数据通信基础知识

根据新版考试大纲，希赛教育专家特别提示：本节考查知识包括：信道特性、传输介质、数据调制与编码技术、数据交换与复用技术。

3.1.1　数据信号和信道的基本概念

通信技术按照信号的传输类型分为模拟通信和数字通信。

在电话通信中，电话线上传送的电信号随着模拟用户声音大小的变化而变化。这个变化的电信号无论在时间上或是在幅度上都是连续的，这种信号称为模拟信号。

在电报通信中，其电报信号是用“点”和“划”组成的电码（叫做莫尔斯电码）来代表文字和数字。如果用有电流代表“1”、无电流代表“0”，那么“点”就是 1，0，“划”就是 1，1，1，0。莫尔斯电码是用一点一划代表 A，用一划三点代表 B，所以 A 就是 101110，B 就是 1110101010……。这种离散的、不连续的信号，称为数字信号。

各种数据终端设备交换数据，就必然要传输信号。信息传输的路径我们称为“信道”。信道可以分为物理信道和逻辑信道。物理信道由传输介质和设备组成，用于传输信号或数据的物理通路，网络中两个节点之间的物理通路称为通信链路。逻辑信道不同的就是信号收、发点之间不存在一条物理上的线路。

在数据通信技术中，人们一方面通过研究新的传输媒介来降低噪声的影响，另一方面则是研究更先进的数据调制技术，以更加有效地利用信道的带宽。因此，这也就引出了一个历年考试常常出现的考点：计算信道的数据速率。信道的数据速率计算公式如图 3-1 所示。

从图 3-1 中，可以看出在计算信道的数据速率时有两种考虑的方式，一是考虑噪声，二是考虑理想传输。

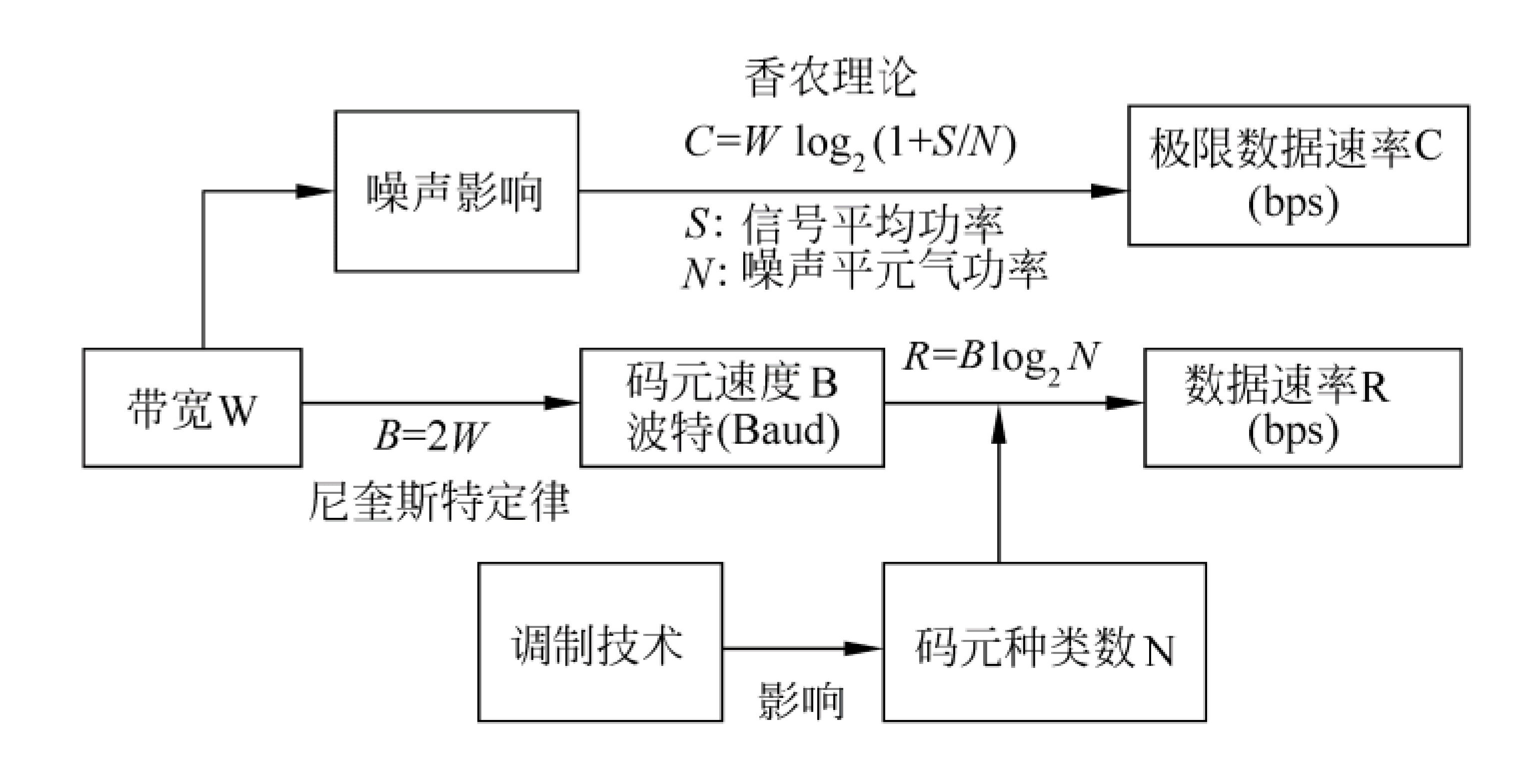


图 3-1　信道的数据速率计算公式

3.1.2　数据通信模型的构成

数据通信模型主要包括数据终端设备和数据通信线路，其中数据终端设备一般有计算机系统和一些其他的终端设备；数据通信线路包括通信信道和数据通信设备。

1．数字通信系统结构

数据通信系统是指以计算机为中心，用通信线路与分布式的数据终端连接起来，执行数据通信的系统。图 3-2 是数据通信系统的一般结构。

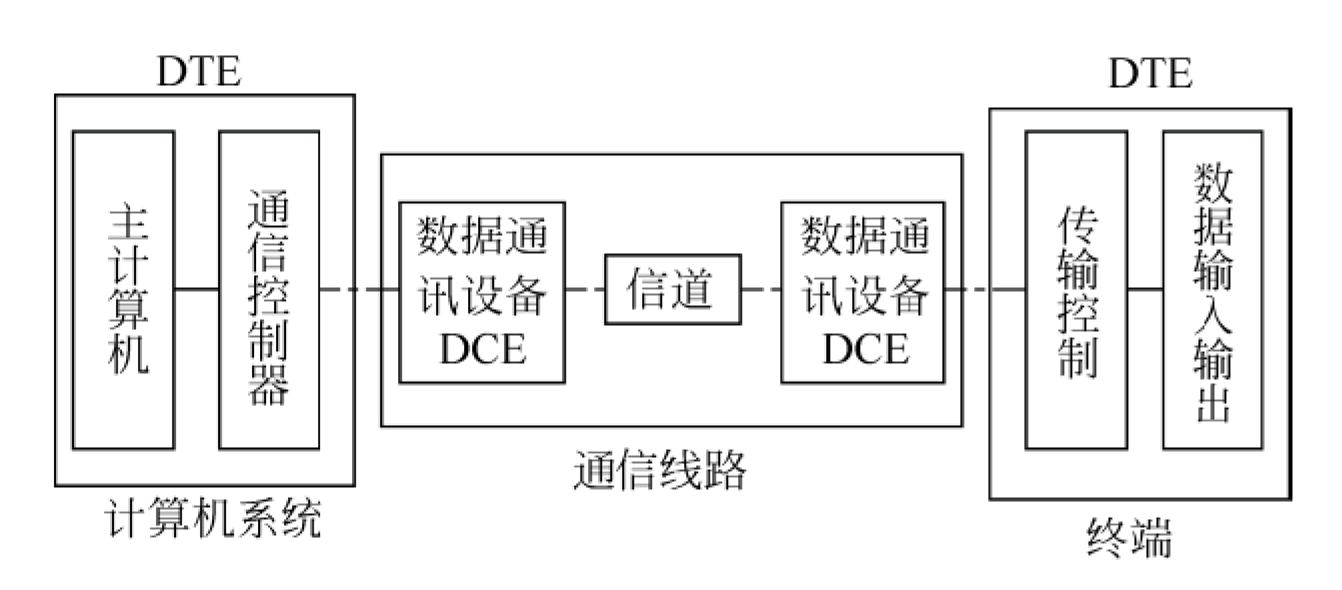


图 3-2　数字通信系统一般结构

计算机系统和终端设备都是数据终端设备 DTE（Date Terminal Equipment），它们都是数据信息的源和目的地，或者既是源又是目的地，是连接在网络上的计算机系统、输入输出设备的总称。但是两者作用不同，终端设备接收来自计算机的数据或向计算机系统发送数据；计算机系统则主要对数据进行收集和处理，是数据处理的核心。DTE 具有根据通信协议控制通信的功能。终端设备除具有数据的输入输出外，还有对线路断开或接通、确认对方状态、发现传输中错误和纠错等控制功能。

通信线路上的设备，如交换机和其他一些中间设备称为数据电路终端设备 DTE（Date Circuit-terminating Equipment）或数据通信设备 DCE（Date Communication Equipment），它们是网络设备的总称。

2．数字通信过程

第一步 建立通信线路。通信对方经过交换设备的许可，建立双方通信的物理通道。

第二步 建立数据传输链路、通信双方相互确认并建立同步联系，使双方设备处于正确收发状态。

第三步 数据传输直到结束。通信双方根据协议通信，并保证正确性。通信结束时候，相互交换终结信息，确认通信结束。

第四步 拆除通信线路。由通信双方之一通知交换设备，通信结束可以拆除线路，切断物理链路。

3.1.3　数据传输基本知识

在通信技术发达的今天，数据传输技术多种多样，本节中主要介绍常见的并串行传输技术、同异步传输技术及数据传输的基本形式。

1．数据传输方式

根据不同的传输标准，数据的传输方式可分为并行传输与串行传输、同步传输与异步传输等等。

1）并行传输与串行传输

（1）并行传输。由 0 和 1 组成的二进制值可以组成 n 比特的位组。计算机使用和生成以比特组为单位的数据，就像我们在英语会话时用词而不是一个个的字母来交流一样。从概念上说，并行传输的机制很简单：一次使用 n 条导线来传输 n 个比特。并行传输的优势在于速度。

（2）串行传输。在串行传输中，比特是一个一个依次发送的，因此在两个通信设备之间传输数据只需要一条通信信道，而不是 n 条。串行传输相对于并行传输的优点是：因为只需要一条通信信道，串行传输的费用大约只是并行传输的 n 分之一。串行传输缺点在于存在一个收、发双方如何保持码组或字符同步的问题，这个问题不解决，接受方就不能从接受到的数据流中正确地区分一个个的字符来，导致传输失去意义。如何解决码组或字符的同步问题，目前有两种不同的方法，即为异步传输方式和同步传输方式。

2）异步传输与同步传输

（1）异步传输。在异步传输方式中，每次传送一个字符（5～8 位），都在每个字符代码前加一起始位，表示该字符代码的开始。在字符和校验码后加一停止位，以示该代码的结束。所以又称起止式同步，起始位编码为“0”，持续 1 位时间，停止位编码为“1”持续 1～2 位。当不发送数据时，发送端连续地发送停止码“1”。接收端一旦接收到从 1 到 0 信号跳变，便知道要开始新字符的发送，利用这种极性的改变便可启动定时机构，实现同步。

当接收到接收停止位，就将定时机构复位，准备接收下一个字符代码。在异步传输中不需要传输时钟脉冲。由于这种方式的字符发送是相互独立的，故称为异步方式。

异步通信设备易于安装，维护简单且价格便宜；但异步方式由于每一个字符都引入起始和停止位，所以开销大、效率低、速率低，常用于低速传输，如 1200bps 或更低的速度。分时终端与计算机的通信一般是异步的。

（2）同步传输。在这种方式中，利用时钟的同步使发送和接收装置之间的定时不发生误差。使时钟保持同步的方法之一，是在接收装置和发送装置之间采用单独的时钟信息，称为同步法。另一种方法是将定时信号包含在数据信号中发送，直接从数据波形本身中提取同步信号，称自同步法。如数字信号利用曼彻斯特编码时，规定传送“0”信号时是先正后负，传送“1”信号时是先负后正。

由于数据信号都是由二进制码按预定规律编排而成，它包含位、字、句及帧。数据传输的代码结构是由若干位组成字，由若干字组成句，由若干句组成帧，传输时不仅位需要同步，其余字、句、帧都要同步，这就叫“群”同步。只有做到群同步，接收端才能正确识别字、句、帧等码群。如果只有位同步而无群同步，收到的信号将是一串无意义的码元序列。为使接收装置能确定数据块的开始和结束，每一数据块前、后用同步数据块加上同步定界符等控制信息的组合，常称为“帧”。帧的实际格式，常取决于传输方案，是面向比特（位）的，还是面向字符方式的。

2．通信双方信息交互方式

从通信双方信息交互的方式来看，可以有以下三种基本方式：

（1）单向通信：又称为单工通信，即只能有一个方向的通信而没有反方向的交互。无线电广播或有线电广播以及电视广播就属于这种类型。

（2）双向交替通信：又称为半双工通信，即通信的双方都可以发送信息，但不能同时发送和同时接受。这种通信方式是一方发送另一方接受，过一段时间后再反过来。许多对讲机使用的就是半双工方式，当一方按下按钮说话时，不能听见对方的声音。

（3）双向同时通信：又称为全双工通信，即通信的双方可以同时发送和接受信息。一般的电话系统和计算机间通信常用全双工方式。

其中单向通信只需要一条信道，而双向交替通信或双向同时通信则都需要两条信道（每个方向各一条）。显然，双向同时通信的传输效率最高。

这里提醒读者注意：有时人们也常用“单工”这个词来表示“双向交替通信”。如常说的“单工电台”并不是只能进行单向通信。正因为如此，国际电信联盟远程通信标准化组才不采用“单工”，“半双工”和“全双工”这些容易弄混的术语作为正式的名词。

3．数据传输的形式

根据传输技术的不同，数据传输形式可分为基带传输、频带传输和宽带传输等三种。

1）基带传输

模拟信号经过信源编码得到的信号为数字基带信号，将这种信号经过码型变换，不经过调制，直接送到信道传输，称为数字信号的基带传输。

2）频带传输

频带传输就是先将基带信号变换（调制）成便于在模拟信道中传输的、具有较高频率范围的模拟信号（称为频带信号），再将这种频带信号在模拟信道中传输。

3）宽带传输

将信道分为多个子信道，分别传送音频、视频和数字信号，称为宽带传输。

一般说，宽带传输与基带传输相比有几个优点：能在一个信道中传输声音、图像和数据信息，使系统具有多种用途；一条宽带信道能划分为多条逻辑基带信道，实现多路复用，因此信道的容量大大增加；宽带传输的距离比基带远，因为基带传输直接传送数字信号，传输的速率越高，能够传输的距离越短。

3.1.4　数据调制与编码

人类在长期的社会活动中需要不断地交往和传递信息。这种传递信息的过程就叫做通信。在通过通信媒体发送信息之前，信息必须形成信号。当将数据由一地传送到另一地时，必须将其转换为信号。那么，信号是如何被传送与接收的呢？

1．模拟信道传送模拟数据

模拟数据可以在模拟信道上直接传送，但在网络数据传送中并不常用，典型的例子是声音在普通电话系统中的传输，电话线中传输的是模拟声音的电信号。人们仍然会对模拟数据进行调整，然后再通过模拟信道发送。模拟数据通过模拟通道传送的调制方式主要有调幅 AM（Amplitude Modulation）、调频 FM（Frequency Modulation）和调相 PM（Phase Modulation）以及正交调幅（QAM）几种方式。

2．数字信道传送模拟数据

模拟信号必须转变为数字信号，才能在数字信道上传送，这个过程称为“数字化”。典型的特例是网络电话。

根据采样定理，为了实现 4000Hz 以下的语音数据传送，每秒采集 8000 个样本则可以描述这个话音。如果样本是使用模拟数据，则能完全描绘。使用数字信号时，必须使用二进制码来描述每个样本，受到二进制码的位数的限制，这个描述必然是近似值，如果使用 8 位比特来描述，则有 256 个值。这种调制方式称为脉码调制 PCM（Pulse Code Modulation）。

3．模拟信道传送数字数据

计算机拨号上网，电话网络传送的是模拟数据，计算机是数字设备只能收发数字数据，这就涉及到模拟信道传送数字信号的变换问题。调制方式有振幅键控（ASK）、移频键控（FSK）、移相键控（PSK）和差分移相键控（DPSK）等。

4．数字信道传送数字数据

在数字信道中传输计算机数据时，要对计算机中的数字信号重新编码进行基带传输。基本的编码方法有极性编码、归零性编码和双相码。

1）极性编码

极包括正极和负极。因此从这里就可以理解单极性码，就是只使用一个极性，再加零电平（正极表示 0，零电平表示 1）；极性码就是使用了两极（正极表示 0，负极表示 1）；双极性码则是使用了正负两极和零电平（其中有一种典型的双极性码是信号交替反转编码 AMI，它用零电平表示 0，1 则使电平在正、负极间交替翻转）。码的极性变化如图 3-3 所示。

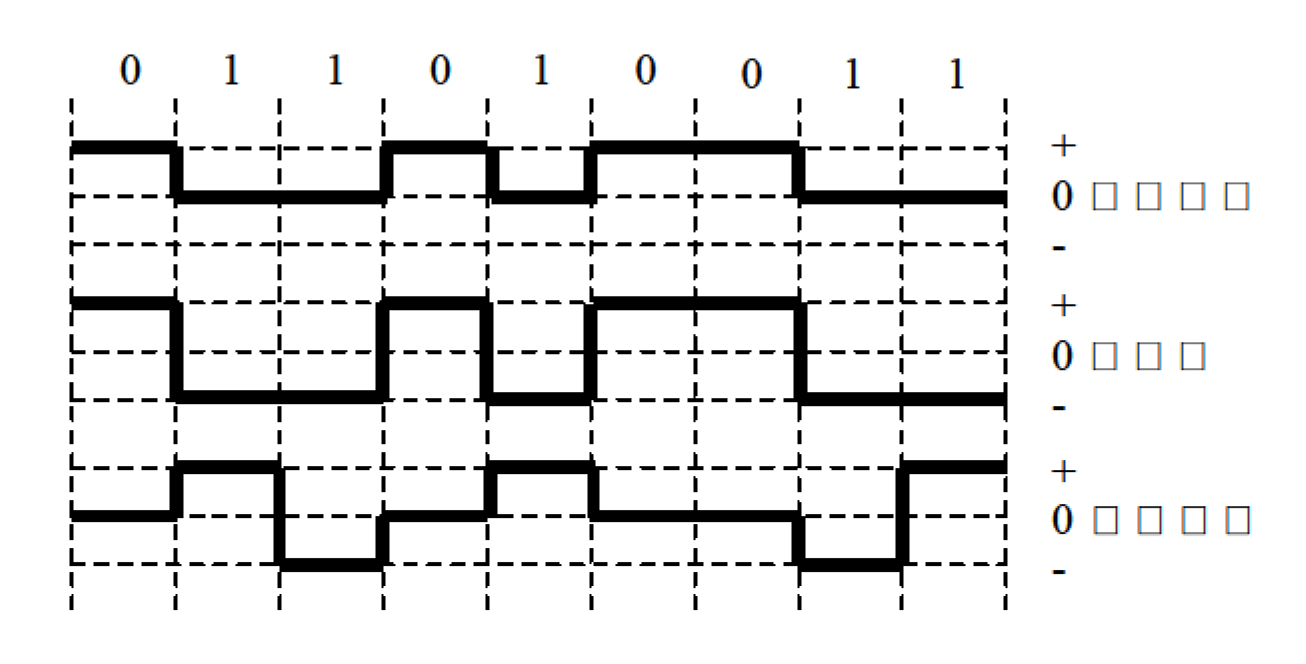


图 3-3　码的极性变化

在极性编码方案中，都是始终使用某一特定的电平来表示特定的数，因此当发送连续多个“1”或“0”时，将无法直接从信号判断出个数。要解决这个问题，就需要引入时钟信号才能够解决这个问题。

2）归零性编码

归零指的是编码信号量不是回归到零电平。归零码是指码元中间的信号回归到 0 电平。不归零码则不回归零（而是当 1 时电平翻转，0 时不翻转），这也称之为差分机制。

3）双相码

通过不同方向的电平翻转（低到高代表 0，高到低代表 1），这样不仅可以提高抗干扰性，还可以实现自同步，它也是曼彻斯特编码的基础。

归零码和双相码如图 3-4 所示。

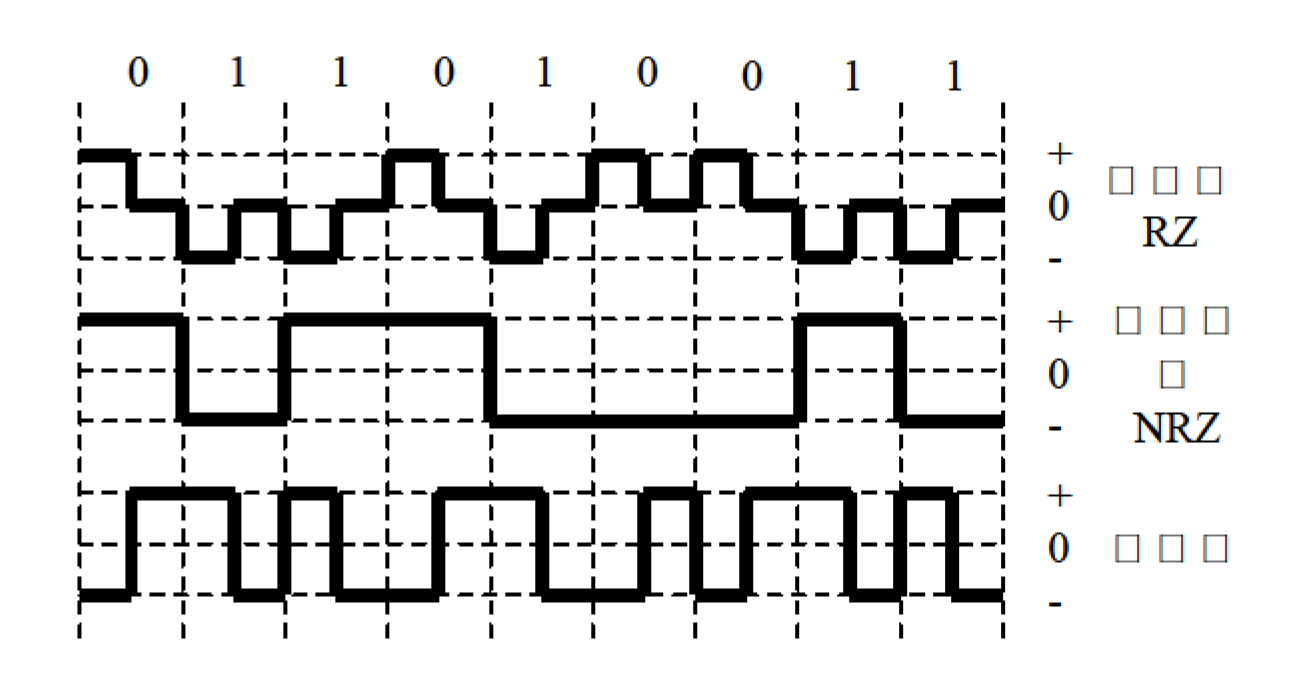


图 3-4　归零码与双相码

应用性编码主要有曼彻斯特编码、差分曼彻斯特编码、4B/5B 编码、8B/6T 编码和 8B/10B 编码等。

1）曼彻斯特编码和差分曼彻斯特编码

曼彻斯特编码和差分曼彻斯特编码如图 3-5 所示。

曼彻斯特编码是一种双相码，用低到高的电平转换表示 0，用高到低的电平转换表示 1（注意：某种教程中关于此部分内容有相反的描述，也是正确的），因此它也可以实现自同步，常用于以太网（802.3 10M 以太网）。

差分曼彻斯特编码是在曼彻斯特编码的基础上加上了翻转特性，遇 0 翻转，遇 1 不变，常用于令牌环网。要注意的一个知识点是：使用曼码和差分曼码时，每传输 1bit 的信息，就要求线路上有 2 次电平状态变化（2 Baud），因此要实现 100Mbps 的传输速率，就需要有 200MHz 的带宽，即编码效率只有 50%。

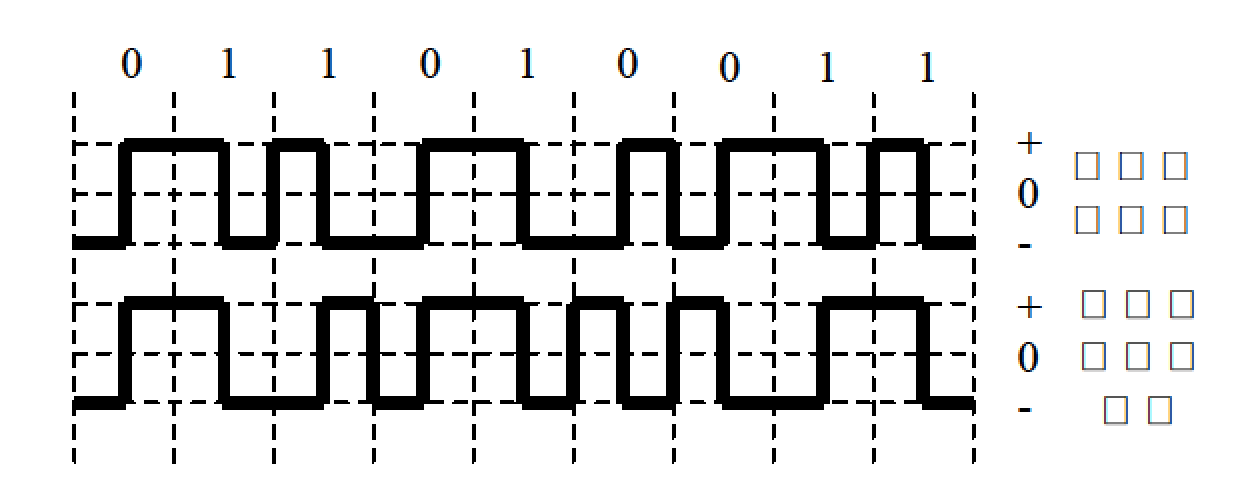


图 3-5　曼彻斯特和差分曼彻斯特编码

2）4B/5B 编码、8B/6T 编码和 8B/10B 编码

正是因为曼码的编码效率不高，导致在带宽资源宝贵的广域网以及速度要求更高的局域网中出现了困难，为了解决这些困难，因此出现了 mBnB 编码，即将 *m* 比特位编码成 *n* 波特（代码位）。

4B/5B 编码、8B/6T 编码和 8B/10B 编码的比较如表 3-1 所示。

表 3-1　应用编码标准

编 码 方 案	说　　明	效　　率	典 型 应 用
4B/5B	每次对 4 位数据进行编码，将其转为 5 位符号	1.25 波特/位 即 80%	100Base-FX、100Base-TX、FDDI
8B/10B	每次对 8 位数据位进行编码，将其转为 10 位符号	1.25 波特/位 即 80%	千兆以太网
8B/6T	8bit 映射为 6 个三进制位	0.75 波特/位	100Base-T4

3.1.5　多路复用技术

多路复用指的是复用信道，即利用一个物理信道同时传输多个信号，以提高信道利用率，使得一条线路能同时由多个用户使用而互不影响。即低速线路在其远端合并，仅

由一条较高速度的线路传输所有信息，而不是在一个发送端和接收端之间连接着许多低速线路。

多路复用的优点在于仅需一条传输线路，所需介质较少，所用的传输介质的容量可以得到充分利用，从而降低了设备费用，提高了工作效率；用户不需要进行任何实际的修改，多路复用系统对用户是透明的，每个很远的地点都好像仍然直接接到总部所在地；由于线路中用的缓冲部件较少，时间延迟较少。

多路复用技术通常分为频分多路复用、时分多路复用、波分多路复用、码分多址和空分多址。

1．频分多路复用

频分复用的典型例子有许多，如无线电广播、无线电视。同样，有线电视也是基于同一原理。总之，频分复用是把线路或空间的频带资源分成多个频段（带），将其分别分配给多个用户，每个用户终端的数据通过分配给它的子通路（频段）传输，主要用于电话和电缆电视（CATV）系统。在 FDM 频分复用中，各个频段（带）都有一定的带宽，称之为逻辑信道（有时简称为信道）。为了防止相邻信道信号频率覆盖造成的干扰，在相邻两个信号的频率段之间设立一定的“保护”带，保护带对应的频谱不被使用，以保证各个频带互相隔离不会交叠。

2．时分多路复用

时分多路复用是将传输信号的时间进行分割，使不同的信号在不同时间内传送，即将整个传输时间分为许多时间间隔（称为时隙、时间片等）。每个时间片被一路信号占用。因为数字信号是有限个离散值，所以适合于采用时分多路复用技术，而模拟信号的传输一般采用频分多路复用。TDM 又分为同步时分复用（STDM）和异步时分复用（ATDM）。

1）同步时分复用

同步时分复用采用固定时间片分配方式，即将传输信号的时间按特定长度连续地划分成特定时间段，再将每一时间段划分成等长的多个时隙（时间片），每个时隙以固定的方式分配给各路数字信号。各路数字信号在每一时间段都顺序分配到一个时隙。

由于在同步时分复用方式中，时隙预先分配且固定不变，无论时间片拥有者是否传输数据都占有一定时隙，形成了时隙浪费，其时隙的利用率很低，为了克服 STDM 的缺点，引入了异步时分复用技术。

2）异步时分复用

异步时分复用技术又被称为统计时分复用或智能时分复用（ITDM），它能动态地按需分配时隙，避免每个时间段中出现空闲时隙。

ATDM 是指有某一路用户有数据要发送时才把时隙分配给它。当用户暂停发送数据时不给它分配线路资源（时隙）。线路的空闲时隙可用于其他用户的数据传输。所以每个用户的传输速率可以高于平均速率（即通过多占时隙），最高可达到线路总的传输能力（即占有所有的时隙）。如线路总的传输能力为 28.8Kbps，3 个用户公用此线路，在同步时分

复用方式中，则每个用户的最高速率为 9600bps，而在 ATDM 方式时，每个用户的最高速率可达 28.8Kbps。

3．波分多路复用

波分复用是频分复用的一种形式，应用于光纤通信中。不同波长的光线通过同一根光纤传播，和频分复用一样，每个信道有自己的频率范围，由于光纤系统使用的衍射光栅是完全无源的，因此极其可靠。由于日常生活中，人们使用颜色来区分不同波长的光波，所以波分复用也称为色分多路复用。

4．码分复用

码分复用与前面介绍的信道分配方法完全不同，不同用户传输信息所用的信号不是靠频率不同或时隙不同来区分，而是用各自不同的编码序列来区分，码分复用允许所有信号同时在整个频段上进行传输，类似于酒会原理，码分复用就是房间里的不同对的人分别用不同的语言进行交谈，讲法语的人只理会法语，其他的就当作噪音不加理会。码分复用的关键就是能够提取出所需的信号，同时将其他的一切当作随机噪声抛弃。

因此，码分复用的关键就是能够提取出所需的信号，同时将其他的一切当作随机噪声抛弃。

5．空分复用

空分复用是指通过信号在空间上的分离来达到信道的复用。

例如，在光纤通信中，空分复用包括两个方面：一是光纤的复用，即将多根光纤组合成束；二是在一根光纤中的光“束”沿空间分割的一种多维通信方式。可以引入多维相干度调制与解调的新概念来实现多路空分复用通信。

3.1.6　数据交换技术

交换技术即转接技术，常用的交换技术有三种：电路交换（线路交换）、报文交换和分组交换（包交换），本节需要掌握的知识点有下面几种交换技术及特点。

1．电路交换

电路交换是一种直接的交换方式，它为一对需要进行通信的装置（站）之间提供一条临时的专用通道，即提供一条专用的传输通道，既可是物理通道又可是逻辑通道（使用时分或频分复用技术）。目前公用电话网广泛使用的交换方式是电路交换，经由电路交换的通信包括三个阶段：

（1）电路建立：通过源站点请求完成交换网中对应的所需逐个节点的连接过程，以建立起一条由源站到目的站的传输通道。

（2）数据传输：现在，信号可以经建立的链路从发送端传送到接收端，通常为全双工传输。

（3）电路拆除：在完成数据或信号的传输后，由源站或目的站提出终止通信，各节点相应拆除该电路的对应连接，释放由原电路占用的节点和信道资源。

电路交换技术的优缺点及其特点如下。

优点：数据传输可靠、迅速，数据不会丢失且保持原来的序列。

缺点：在某些情况下，电路空闲时的信道容易被浪费；在短时间数据传输时电路建立和拆除所用的时间得不偿失，因此，它适用于系统间要求高质量的大量数据传输的情况。

特点：在数据传送开始之前必须先设置一条专用的通路。在线路释放之前，该通路由一对用户完全占用。对于猝发式的通信，电路交换效率不高。

2．报文交换

报文交换方式的数据传输单位是报文，报文就是站点一次性要发送的数据块，其长度不限且可变。当一个站点要发送报文时，它将一个目的地址附加到报文上，网络节点根据报文上的目的地址信息，把报文发送到下一个节点，一直逐个节点地转送到目的节点。

每个节点在收到整个报文并检查无误后，就暂存这个报文，然后利用路由信息找出下一个节点的地址，再把整个报文传送给下一个节点。因此，端与端之间无需先通过呼叫建立连接。一个报文在每个节点的延迟时间，等于接收报文所需的时间加上向下一个节点转发所需的排队延迟时间之和。

1）报文交换的特点

报文从源点传送到目的地采用“存储-转发”方式，在传送报文时，一个时刻仅占用一段通道。在交换节点中需要缓冲存储，报文需要排队，故报文交换不能满足实时通信的要求。

2）报文交换的优点

电路利用率高。由于许多报文可以分时共享两个节点之间的通道，所以对于同样的通信量来说，对电路的传输能力要求较低。在电路交换网络上，当通信量变得很大很大时，就不能接受新的呼叫。而在报文交换网络上，通信量大时仍然可以接收报文，不过传送延迟会增加。报文交换系统可以把一个报文发送到多个目的地，而电路交换网络很难做到这一点。

3）报文交换的缺点

不能满足实时或交互式的通信要求，报文经过网络的延迟时间长且不定。有时节点收到过多的数据而无空间存储或不能及时转发时，就不得不丢弃报文，而且发出的报文不按顺序到达目的地。

3．分组交换

分组交换属于“存储/转发”交换方式，但它不像报文交换那样以报文为单位进行交换、传输，而是以更短的、标准的“报文分组”（Packet，包）为单位进行交换传输。分组是一组包含数据和呼叫控制信号的二进制数，把它作为一个整体加以转接，这些数据、呼叫控制信号以及可能附加的差错控制信息是按规定的格式排列的。

交换网可采用两种方式：数据报传输分组交换或虚电路传输分组交换进行交换。

1）数据报传输分组交换

交换网把进网的任一个分组都当作单独的“小报文”来处理，而不管它属于哪个报文的分组，就像报文交换中把一份报文进行单独处理一样。上述这种分组交换方式简称为数据报传输方式，作为基本传输单位的“小报文”被称为数据报（Datagram）。

2）虚电路传输分组交换

所谓虚电路就是两个用户的终端设备在开始互相发送和接收数据之前需要通过通信网络建立逻辑上的连接，一旦这种连接建立，直至用户不需要发送和接收数据时清除这种连接。

所有分组都必须沿着事先建立的虚电路传输，存在一个虚呼叫建立阶段和拆除阶段（清除阶段）。与电路交换相比，并不意味着实体间存在像电路交换方式那样的专用线路，而是选定了特定路径进行传输，分组所途经的所有节点都对这些分组进行存储/转发，这是与电路交换的实质上的区别。

4．高速交换技术

传统的交换技术不能满足多媒体业务应用，目前提高交换速度的方案有帧中继和 ATM 等。目前流行的交换技术是 ATM（异步传输模式），它是电路交换与分组交换技术的结合，能最大限度地发挥电路交换与分组交换技术的优点，具有从实时的话音信号到高清晰度电视图像等各种高速综合业务传输能力。

3.2　计算机网络基础知识

从历次考试试题来看，计算机网络基础知识是网络管理员考试的一个次重点，也是学习后续章节中的基础。根据对考试大纲的解读，及历年的出题规律，可以总结出本节主要考查知识点包括以下几个方面：OSI 参考模型与各层数据封装、协议层次关系、底层协议（ARP、RARP、HDLC、X.25 等）、网络层与传输层协议（TCP、UDP、IP）、应用层协议（HTTP/HTTPS、SMTP、FTP）等知识。

3.2.1　计算机网络的定义

目前对于计算机网络的精确定义并未统一，关于计算机网络最简单的定义是：一些互相连接的、自治的计算机的集合。若按此定义，则早期的面向终端的网络都不能算是计算机网络，而只能称为联机系统（因为那时候的许多终端都不能算是自治的计算机）。但随着硬件价格的下降，许多终端都具有一定的智能，因而“终端”和“自治的计算机”逐渐失去严格的界限。因此。若用微型计算机作为终端使用，按上述定义，则早期的那种面向终端的网络业可称为计算机网络。最简单的计算机网络就只有两台计算机和链接他们的一条链路，即两个节点和一条链路。

3.2.2 计算机网络的分类和构成

1．计算机网络的分类

计算机网络的分类方法有多种，可以根据网络的用途、覆盖的地理范围、使用的技术等进行分类。

1）按距离分类

根据网络的作用范围，可将网络划分为：

- 局域网（Local Area Network，LAN）：作用范围通常为几米到几十公里。
- 广域网（Wide Area Network，WAN）：作用范围通常为几十公里到几千公里。
- 城域网（Metropolitan Area Network，MAN）：作用范围界于局域网与广域网之间。

2）按通信介质分类

根据通信介质的不同，可将网络划分为：

- 有线网：采用同轴电缆、双绞线、光纤等物理介质传输数据。
- 无线网：采用卫星、微波等无线形式传输数据。

3）按通信传播方式分类

根据通信传播方式的不同，可将网络划分为：

- 点对点网络：网络中成对的主机之间存在着若干对的相互连接关系。
- 广播式网络：网络中只有单一的通信信道，由这个网络中所有的主机共享。

4）按通信速率分类

根据通信速率的不同，可将网络划分为：

- 低速网：数据传输速率在 1.5Mbps 之下。
- 中速网：数据传输速率在 1.5Mbps 至 50Mbps 之间。
- 高速网：数据传输速率在 50Mbps 之上。

5）按使用范围分类

根据使用范围的不同，可将网络划分为：

- 公用网：为社会公众提供服务。
- 专用网：只为一个或几个部门提高服务，不向社会公众开放。

6）按网络控制方式分类

根据网络控制方式的不同，可将网络划分为：

- 集中式网络：网络的处理控制功能高度集中在一个或少数几个节点上，这些节点是网络的处理控制中心，所有的信息流都必须经过这些节点之一，而其余的大多数节点则只有较少的处理控制功能。
- 分布式网络：网络中不存在一个处理控制中心，各个节点均以平等地位相互协调工作和交换信息。

2．计算机网络的构成

任何计算机网络都由网络硬件、网络软件和网络资源组成。

（1）网络硬件：包括网络中的计算机、通信设备和通信介质等。网络中的计算机通常可划分为服务器和客户机两大类。通信设备主要包括网卡、集线器、交换机、重发器、网桥等。通信介质主要包括电缆、光纤、连接转接轴等。

（2）网络软件：包括网络操作系统、网络通信软件、网络协议和协议软件、网络管理及网络应用软件等。

（3）网络资源：包括文本、图像、声音、视频文件和各类数据库等。

从逻辑上看，也可认为计算机网络是由通信子网和资源子网构成的，通信子网面向通信控制和通信处理，资源子网则包括拥有资源的用户主机和请求资源的用户终端。

3.2.3　开放系统互连参考模型

世界上不同年代、不同厂家、不同型号的计算机系统千差万别，将这些系统互联起来就要求彼此开放，也就是要遵守共同的规则与约定（一般称协议）。1977 年，国际标准化组织（ISO）为适应网络标准化发展的需求，在研究、吸取了各计算机厂商网络体系标准化经验的基础上，制定了开放系统互联参考模型（OSI/RM），从而形成了网络体系结构的国际标准。

对于本节知识点的考查，希赛教育专家特别提示：关键在于各层结构特点、封装特性，代表性协议及其关键特性，主要是记忆型与理解型题目。

1．OSI 参考模型结构

OSI 构造了由底向上的七层模型，即物理层（Physical Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、传输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）和应用层（Application Layer），如表 3-2 所示。不同系统同层之间按相应协议进行通信，同一系统不同层之间通过接口进行通信。只有最底层物理层完成物理数据传递，其他同等层之间的通信称为逻辑通信，其通信过程为将通信数据交给下一层处理，下一层对数据加上若干控制位后再交给它的下一层处理，最终由物理层传递到对方系统物理层，再逐层向上传递，从而实现对等层之间的逻辑通信。一般用户由最上层的应用层提供服务。

表 3-2　OSI/RM 层次结构

7．应用层（Application Layer）
6．表示层（Presentation Layer）
5．会话层（Session Layer）
4．传输层（Transport Layer）
3．网络层（Network Layer）
2．数据链路层（Data Link Layer）
1．物理层（Physical Layer）

2．OSI 参考模型各层的功能

OSI 参考模型通过采用分层的结构，把复杂的数据传输过程分解成相对简单的七个层次，并对每一个层次定义相应的功能，以实现对数据传输过程中的各个阶段的控制，下面分别介绍每层的特性和功能。

（1）应用层：是 OSI 参考模型的最高层，应用层确定进程之间通信的性质以满足用户的需要；负责用户信息的语义表示，并在两个通信者之间进行语义匹配。就是说应用层不仅要提供应用进程所需要的信息交换和远程操作，而且还要作为互相作用的应用进程的用户代理（user agent），来完成一些为进行语义上有意义的信息交换所必需的功能。在这一层中，除了广为使用的 HTTP（Hypertext Transfer Protocol，超文本传输协议）、FTP（File Transfer Protocol，文件传输协议）、Telnet（远程登录）、SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）、POP（Post Office Protocol，邮局协议）、DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）、SNMP（Simple Network Manage Protocol，简单网络管理协议）外，随着多媒体技术的发展，RSTP（Real Time Streaming Protocol，实时流传输协议）等多媒体视频点播协议也属于应用层协议。

（2）表示层：提供端到端的信息传输。处理的是 OSI 系统之间用户信息的表示问题。在 OSI 中，端用户（应用进程）之间传送的信息数据包含语义和语法两个方面。语义是信息数据的内容及其含义，它由应用层负责处理。语法是与信息数据表示形式有关的方面，例如信息的格式、编码、数据压缩等。表示层主要用于处理应用实体面向交换的信息的表示方法。这样即使每个应用系统有各自的信息表示法，但被交换的信息类型和数值仍能用一种共同的方法来表示。它包含用户数据的结构和在传输时的比特流或字节流的表示。

（3）会话层：会话层虽然不参与具体的数据传输，但它对数据进行管理，它向互相合作的表示进程之间提供一套会话设施，组织和同步它们的会话活动，并管理它们的数据交换过程。这里，“会话”的意思是指两个应用进程之间为交换面向进程的信息而按一定规则建立起来的一个暂时联系。

（4）传输层：任务是根据通信子网的特性最佳地利用网络资源，并以可靠和经济的方式为两个端系统的会话层之间建立一条传输连接，透明地传输报文。传输层向上一层提供一个可靠的端到端的服务，使会话层不知道传输层以下的数据通信的细节。传输层只存在于端系统（主机）中，传输层以上层就不再管信息传输问题了。代表性协议有 TCP、UDP、SPX 等。

（5）网络层：网络中通信的两个计算机之间可能要经过许多个节点和链路，还可能经过几个通信子网。网络层数据的传送单位是分组（packet），网络层的任务就是要选择合适的路由，使发送站的运输层发下来的分组能够正确无误的按照地址找到目的站并交付目的站的运输层，这就是网络层的寻址功能。对于广播信道构成的通信子网，路由问题很简单，因此这种子网的网络层非常简单，甚至没有。对于通信子网来说，最多只到

网络层。代表性协议有 IP、IPX 等。

（6）数据链路层：负责在两个相邻的节点间的线路上无差错的传送以帧为单位的数据，每一帧包括一定的数据和必要的控制信息，在接收点接收到数据出错时要通知发送方重发，直到这一帧无误地到达接收节点。数据链路层就是把一条有可能出错的实际链路变成让网络层看来好像不出错的链路。代表性协议有 IEEE 802.3/802.2、HDLC、PPP、ATM 等。

（7）物理层：提供相邻设备间的比特流传输。它是利用物理通信介质，为上一层（数据链路层）提供一个物理连接，通过物理连接透明地传输比特流。所谓透明传输指经实际电路后传送的比特流没有变化，任意组合的比特流都可以在这个电路上传输，物理层并不知道比特的含义。物理层要考虑的是如何发送“0”和“1”，以及接收端如何识别。代表性协议有 RS232、V.35、RJ-45、FDDI 等。

3．服务访问点

在同一系统中相邻两层的实体进行交互（即交换信息）的地方，通常称为服务访问点 SAP。

（*N*）层实体向（*N*+1）层实体提供服务，（*N*+1）层实体向（*N*）层实体请求服务，从概念上讲，这是通过位于（*N*）层和（*N*+1）层的界面上的服务访问点（*N*）SAP 来实现的，（*N*）SAP 是一个访问工具，由一组服务元素和抽象操作组成，并由（*N*+1）实体在该点调用。我们把（*N*）层中提供（*N*）服务的那些（*N*）实体总称为（*N*）服务提供者；而把调用（*N*）服务的（*N*+1）实体称为（*N*）服务用户。

3.2.4　TCP/IP 协议体系结构

虽然 OSI/RM 已成为计算机通信体系结构的标准模型，但因 OSI/RM 的结构过于复杂，实际系统中采用 OSI/RM 的并不多。

目前使用最广泛的可互操作的网络体系结构是 TCP/IP 协议体系结构。

1．TCP/IP 模型结构

TCP/IP 协议集由 Internet 工作委员会发布并已成为互联网标准。与 OSI 七层模型结构不同，从不存在正式的 TCP/IP 层次结构模型，但可根据已开发的协议标准和通信任务将其分成 4 个比较独立的层次，如表 3-3 所示。

表 3-3　TCP/IP 层次结构

4. 应用层
3. 传输层
2. 网络互联层（IP 层）
1. 网络接口层（网络访问层）

2．TCP/IP 模型各层的功能

（1）网络接口层：大致对应于 OSI 模型的数据链路层和物理层，TCP/IP 协议不包含

具体的物理层和数据链路层，只定义了网络接口层作为物理层的接口规范。网络接口层处在 TCP/IP 协议的最底层，主要负责管理为物理网络准备数据所需的全部服务程序和功能。该层处理数据的格式化并将数据传输到网络电缆，为 TCP/IP 的实现基础，其中可包含 IEEE 802.3 的 CSMA/CD、IEEE 802.5 的 TokenRing 等。

（2）网络互联层：也称网络层或互联网层，负责将数据报独立地从信源传送到信宿，主要解决路由选择、阻塞控制和网络互联等问题，在功能上类似于 OSI 体系结构中的网络层。网络互联层是 TCP/IP 体系结构的核心，该层最重要的协议称为 IP 协议（Internet Protocol），因此网络互联层又称 IP 层。

（3）传输层：负责在源主机和目的主机之间提供端到端的数据传输服务，相当于 OSI 体系结构中的传输层。本层主要定义了两个传输协议，一个是可靠的、面向连接的传输控制协议（TCP），另一个是不可靠的、无连接的用户数据报协议（UDP）。TCP 和网络层的 IP 协议是互联网中的两个最重要的协议，以至于 TCP/IP 体系结构和 TCP/IP 协议集就以这两个协议的名称来命名。

（4）应用层：包含了所有的高层协议，常见的如简单网络管理协议（SNMP）、超文本传输协议（HTTP）、文件传输协议（FTP）、简单邮件传输协议（SMTP）、域名服务（DNS）和远程终端访问协议。

TCP/IP 协议集作为一种十分流行的网络体系结构，已成为事实上的工业标准。但是 TCP/IP 体系结构没有明显地区分每一层中“服务”、“接口”与“协议”的概念，各层中“接口”与“层”之间的区分也太模糊。TCP/IP 的各层与 OSI/RM 的层次对应关系如表 3-4 所示，但这种对应关系并不是十分严格。

本节只介绍 TCP/IP 体系结构中的网络互联层和传输层的主要协议。与网络接口层有关的协议和应用层协议的介绍请参看本书后续章节。

表 3-4 OSI/RM 与 TCP/IP 的层次对应关系

OSI/RM	TCP/IP
应用层	应用层
表示层	
会话层	
传输层	传输层
网络层	网络互联层
数据链路层	网络接口层
物理层	

3．IP 协议

IP 协议是 TCP/IP 协议集的核心，传输层上的数据信息和网络层上的控制信息都以 IP 数据报的形式传输，IP 协议实现的是无连接、不可靠的数据报服务。

1）IP 地址

为区别 Internet 上几百万台计算机、成千上万的组织和上亿用户，必须给 Internet 上每台计算机（或路由器）与 Internet 的每个接口规定一个唯一的地址，即 IP 地址。

IP 地址是一个 32 位（bit）的二进制数。为了书写和记忆的方便，通常将 IP 地址分为 4 字节（byte），每个字节用一个十进制数来表示，字节之间用圆点分隔，这就是点分十进制表示。例如 IP 地址：

11000000101010001100100010000000

可分成 4 字节：

11000000 10101000 11001000 10000000

每字节用十进制数来表示，字节之间用圆点分隔，表示为 192.168.200.128。

每个 IP 地址由两部分组成：网络标识（NetID）和主机标识（HostID）。网络标识用于唯一标识一个网络，主机标识则确定了某一网络上的某一台主机。为保证 IP 地址的唯一性，专门设立了一个权威机构 InterNIC（Internet Network Information Center）负责 IP 地址的管理。InterINC 只分配 IP 地址中的网络标识，主机标识由各个网络的管理员负责分配。

网络部分所占位数决定了整个互联网最多可以有多少个网络，而主机标识所占位数则决定了一个网络中最多可有多少台主机。由于 Internet 上网络规模有很大区别，IP 地址空间被划分为 5 类，每类具有不同位数的网络标识和主机标识：A 类地址分配给少数规模很大的网络；B 类地址分配给中等规模的网络；C 类地址分配给小规模的网络；D 类地址用于组播（Multicast）业务，E 类地址作为保留。IP 地址编码分类如表 3-5 所示。

表 3-5　IP 地址编码分类

<table>
<tr><td></td><td>0</td><td>1</td><td>2</td><td>3</td><td></td><td>8</td><td>16</td><td>24</td><td>31</td></tr>
<tr><td>A 类</td><td>0</td><td colspan="4">网络标识（7 位）</td><td colspan="4">主机标识（24 位）</td></tr>
<tr><td>B 类</td><td>1</td><td>0</td><td colspan="4">网络标识（14 位）</td><td colspan="3">主机标识（16 位）</td></tr>
<tr><td>C 类</td><td>1</td><td>1</td><td>0</td><td colspan="4">网络标识（21 位）</td><td colspan="2">主机标识（8 位）</td></tr>
<tr><td>D 类</td><td>1</td><td>1</td><td>1</td><td>0</td><td colspan="5">组播</td></tr>
<tr><td>E 类</td><td>1</td><td>1</td><td>1</td><td>1</td><td colspan="5">保留</td></tr>
</table>

根据上述编址规则，IP 地址的第 1 字节，A 类为 0～127，B 类为 128～191，C 类为 192～223，D 类为 224～239，E 类为 240～255。

需要记住以下几种特殊的 IP 地址：

- 网络地址：主机号全 0 表示网络地址（不能做目标地址）。
- 广播地址：主机号全 1 表示广播地址（不能做源地址）。
- 保留地址：为了满足内网的使用需求，保留了一部分不在公网使用的 IP 地址，如表 3-6 所示。

表 3-6 三类私有保留地址

类 别	IP 地址范围	网 络 号	网 络 数
A	10.0.0.0～10.255.255.255	10	1
B	172.16.0.0～172.31.255.255	172.16～172.31	16
C	192.168.0.0～192.168.255.255	192.168.0～192.168.255	255

- 回送（Loopback）地址：为了方便测试，有一个表示本机的特殊保留地址：127.0.0.1。

2）子网及子网掩码

在实际应用中，仅靠网络标识来划分网络会有许多问题。例如某大学的 B 类网络最多允许接入 65 534 台计算机，但实际上不可能将这么多计算机都连接到一个单一的网络中。如果按照学院划分为十多个子网，每个子网最多只允许接入几千台计算机，会给网络寻址和管理带来很大方便。

在一个网络中引入子网，就是将主机标识进一步划分为子网标识和主机标识，通过灵活定义子网标识的位数，可以控制每个子网的规模。例如在上面的例子中，将子网标识位数定为 4，则划分为 16 个子网，每个子网最多允许接入 4094 台计算机。

注意子网划分会导致实际可分配 IP 地址数目减少。例如上面例子中子网划分前的可分配 IP 地址为 65 534，划分后的可分配 IP 地址为 65 504（4094×16），减少了 30 个。但这点损失与子网划分所带来的巨大收益相比是微不足道的。

判断两台机器是否在同一个子网内，需要用到子网掩码。子网掩码同 IP 地址一样，也是一个 32 位的二进制数，但其网络标识和子网标识部分全为 1，主机标识部分全为 0。例如上面例子的子网掩码为 11111111 11111111 11110000 00000000，即 255.255.240.0。

判断两个 IP 地址是不是在同一个子网内，只要判断这两个 IP 地址与子网掩码做逻辑“与”的结果是否相同即可。例如在上面的例子中，设 IP 地址 A，B，C 分别为 190.78.240.1、190.78.250.1、190.78.230.1。将 A，B，C 分别转换为二进制表示形式：

10111110 01001110 11110000 00000001

10111110 01001110 11111010 00000001

10111110 01001110 11100110 00000001

与子网掩码 11111111 11111111 11110000 00000000 逻辑“与”的结果分别为：

10111110 01001110 11110000 00000000

10111110 01001110 11110000 00000000

10111110 01001110 11100000 00000000

因此 IP 地址 190.78.240.1 与 190.78.250.1 在一个子网内，而 IP 地址 190.78.240.1 与 190.78.230.1 不在一个子网内。

3）IP 数据报格式

IP 协议的数据报格式如图 3-6 所示。

0	4	8	16			19　　24　　31
版本号	首部长度	区分服务	报文总长度			
标识				DF	MF	分片偏移量
生存时间		协议	首部校验和			
源IP地址						
目的IP地址（可选）						
IP选项与填充数据						
用户数据 ……						

图 3-6　IP 数据报格式

- “版本号”：指明所用 IP 协议的版本号，如 IPv4 或 IPv6。
- “首部长度”：以 4 字节为单位，例如长度为 5 表示 20 字节。
- “区分服务”：可选择最小延迟、最大吞吐量、最高可靠性和最小花费之一。
- “报文总长度”：理论上 IP 数据报的最大长度可达 65 535 字节，但考虑到传输时延和主机的处理能力，多数机器将此长度限制在 576 字节之内。
- “标识”：发送方每发送一个数据报，其数据报标识就加 1。若数据报在传输过程中被分成较小的数据段时，每个数据段必须携带其所属数据报的数据报标识，接收方据此可将属于同一个数据报的数据段重新组装成数据报。
- “DF”（Don't Fragment）：指示路由器是否将数据报分段。
- “MF”（More Fragment）：标识该数据段的后面还有没有其他数据段，即该数据段是不是数据报的最后一个数据段。
- “分片偏移量”：表示该数据段在数据报中的位置，以 8 字节作为基本单位。
- “生存时间”（Time to live）：用来限制数据报的寿命。数据报每到达一个路由器该字段即减 1，减至 0 时数据报将被丢弃。
- “协议”：指明传输层使用的协议（如 TCP 或 UDP）。
- “首部校验和”：用于对数据报头进行校验。

4．ARP 协议与 RARP 协议

ARP 协议主要负责将局域网中的 32 位 IP 地址转换为对应的 48 位物理地址，即网卡的 MAC 地址，比如 IP 地址为 192.168.0.1 网卡 MAC 地址为 00-03-0F-FD-1D-2B。整个转换过程是一台主机先向目标主机发送包含 IP 地址信息的广播数据包，即 ARP 请求，然后目标主机向该主机发送一个含有 IP 地址和 MAC 地址的数据包，通过 MAC 地址两个主机就可以实现数据传输了。

在安装了以太网网络适配器的计算机中都有专门的 ARP 缓存，包含一个或多个表，用于保存 IP 地址以及经过解析的 MAC 地址。在 Windows 中要查看或者修改 ARP 缓存中的信息，可以使用 arp 命令来完成，比如在 Windows XP 的命令提示符窗口中输入“arp –a”或“arp –g”可以查看 ARP 缓存中的内容；输入“arp -d IPaddress”表示删除指定的 IP 地址项（IPaddress 表示 IP 地址）。arp 命令的其他用法可以通过输入“arp /?”查看到。

RARP 反向地址转换协议允许局域网的物理机器从网关服务器的 ARP 表或者缓存上请求其 IP 地址。网络管理员在局域网网关路由器里创建一个表以映射物理地址（MAC）和与其对应的 IP 地址。

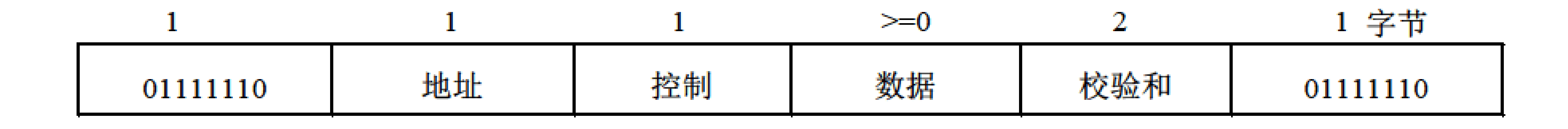
5．ICMP 协议

ICMP 协议（Internet Control Message Protocol）通常被认为是网络互联层的协议，更确切地说，是工作在 IP 协议之上又不属于传输层的协议。网络互联层和传输层的协议实体调用 ICMP 消息来传送一些控制信息，ICMP 消息是封装在 IP 数据报中传输的。

ICMP 消息有询问消息和错误消息两类。询问消息用来请求一些信息，如无盘工作站的子网掩码或远程主机的应答等，通常采用请求-应答模式进行交互。错误消息只用来报告错误，不需要应答。

6．HDLC 协议

HDLC 帧格式包括标志字段、地址字段、控制字段、数据和校验和。HDLC 协议的帧格式如图 3-7 所示。



1	1	1	>=0	2	1 字节
01111110	地址	控制	数据	校验和	01111110

图 3-7　IP 数据报格式

标志字段（01111110）：用于确定帧的起始和结束，以进行帧同步和准确识别长度可变的帧。

在两个标志字段之间的比特串中，如果碰巧出现了和标志字段一样的组合，就会被误认为是帧边界。为了避免这种错误，HDLC 采用比特填充法使一个帧中两个标志字段之间不会出现 6 个连续的 1。具体做法是：在发送端，在加标志字段之前，先对比特串扫描，若发现 5 个连续的 1，立即在其后加一个 0。在接收端收到帧后，去掉头尾的标志字段，对比特串进行扫描，当发现 5 个连续的 1 时，立即删除其后的 0，这样就还原成原来的比特流了。

7．TCP 与 UDP 协议

传输层上有两个主要的协议：一个是可靠的、面向连接的传输控制协议（TCP），另一个是不可靠的、无连接的用户数据报协议（UDP）。

TCP 为传输控制协议，是一个面向连接的协议，它提供双向的、可靠的、有流量控

制的字节流的服务。字节流服务的意思是，在一个 TCP 连接中，源节点发送一连串的字节给目的节点。可靠服务是指数据有保证的传递、按序、没有重复。发送方 TCP 实体将应用程序的输出不加分隔地放在数据缓冲区中，输出时将数据块划分成长度适中的段，每个段封装在一个 IP 数据报中传输。

UDP 是一种简单的面向数据报的传输协议，实现的是不可靠、无连接的数据报服务，通常用于不要求可靠传输的场合，可以提高传输效率，减少额外开销。使用 UDP 传输时，应用进程的每次输出均生成一个 UDP 数据报，并将其封装在一个 IP 数据报中发送。

3.2.5　网络传输介质

对于本知识点来说，主要是要求能够了解各种常见的传输介质的特性，如传输介质的最大传输距离、数据传输速率等，以及它们之间的横向比较。不过值得注意的是，在网络管理员考试下午模块中，通常在第一大题中，也还会有一些与传输介质相关的问题（例如，在网络拓扑中，如何选择适当的传输介质），这就要求考生对常见传输介质的特性、性价比要有综合考虑。

1．双绞线

双绞线（Twisted Pair，TP）是目前计算机网络综合布线中最常用的一种传输介质。双绞线由一对一对的带绝缘塑料保护层的铜线组成。每对绝缘的铜导线按一定密度互相绞在一起，可有效的降低信号干扰的程度，每一根导线在传输中辐射的电波会被另一根线上发出的电波抵消。目前，双绞线可分为非屏蔽双绞线（Unshielded Twisted Pair，UTP）和屏蔽双绞线（Shielded Twisted Pair，STP）。其中屏蔽双绞线的外层都是由一层铝箔包裹的，可以有效的减小辐射，当然也不能完全消除辐射。屏蔽双绞线的价格相对非屏蔽双绞线来说稍微昂贵些，安装也比非屏蔽双绞线难一些。类似于同轴电缆，它必须配有支持屏蔽功能的特殊连接器和相应的安装技术。但它有较高的传输速率，100m 内可达到 155Mbps。

双绞线的包括如下几种物理特性：

（1）衰减：衰减是沿链路的信号损失度量。衰减与线缆的长度相关，随着长度的增加，信号衰减也随之增加。衰减用分贝 dB 为单位，表示源传送端信号到接收端信号强度的比率。

（2）近端串扰（NEXT）：当电流在一条导线中流通时，会产生一定的电磁场，干扰相邻导线上的信号。频率越高这种影响就越大。双绞线就是利用两条导线绞合在一起后，因为相位相差 180°的原因而抵消相互间的干扰的。绞距越紧则抵消效果越佳，也就越能支持较高的数据传输速率。

（3）直流电阻：直流环路电阻会消耗一部分的信号，并将其转变成热量。它是指一对导线电阻的和。

（4）特性阻抗：与环路直流电阻不同，特性阻抗包括电阻及频率为 1MHz～100MHz

的电感阻抗，它与一对电线间的距离及绝缘体的电气性能有关。

（5）衰减串扰比（ACR）：它由最差的衰减量与 NEXT 量值的差值计算出。ACR 值较大时，表示抗干扰的能力更强。一般要求大于 10dB。

2．同轴电缆

同轴电缆中用于传输信号的铜芯和用于屏蔽的导体是共轴的，同轴之名由此而来。同轴电缆从用途上分可分为基带同轴电缆（粗同轴电缆）和宽带同轴电缆（细同轴电缆）。其中基带同轴电缆的屏蔽层是用铜做成的网状层，特征阻抗为 50Ω，用于数字传输。而宽带同轴电缆的屏蔽层是由铝箔构成的，特征阻抗为 75Ω，用于模拟传输。

3．光纤

光纤全称“光导纤维”。光纤是由前香港中文大学校长高锟提出并发明。1970 年美国康宁公司首先研制出衰减为 20dB / km 的单模光纤，从此以后，世界各国纷纷开展光纤研制和光纤通信的研究，并得到了广泛的应用。

光纤是一种由玻璃或塑料制成的纤维，利用光的全反射原理而进行光传导的介质。是一种外包了一层保护层的、横截面积非常小的双层同心圆柱体。

根据光纤纤芯直径的粗细，可将光纤分为多模光纤（Multi-mode Fiber，MMF）和单模光纤（Single-mode Fiber，SMF）两种。单模光纤与多模光纤的比较如表 3-7 所示。

表 3-7 单模光纤与多模光纤的比较

项 目	单模光纤	多模光纤
距离	长	短
数据传输速率	高	低
光源	激光	发光二极管
信号衰减	小	大
端接	较难	较易
造价	高	低

4．无线传输媒介

无线传输媒介主要包括无线电波、微波和红外线。

（1）无线电波：需要专用的频率，易被窃听。

（2）微波：可分为地面微波和卫星微波，带宽高、容量大，但受天气影响大。

（3）红外：设备便宜、带宽高，但传输距离有限，易受室内空气状态影响。

3.2.6 网络互联设备

常见的网络互联设备包括中继器（集线器、无线 AP）、网桥、路由器、网关及网络适配器（网卡）。以上是从 OSI 协议层出发的概念分类，实际上在市面上的设备都是多功能组合，向下兼容的。表 3-8 则是对以上设备的一个总结。

表 3-8　网络互关设备

互 联 设 备	工 作 层 次	主 要 功 能
中继器	物理层	对接收信号进行再生和发送，只起到扩展传输距离的作用，对高层协议是透明的，但使用个数有限（以太网是 4 个）
网桥	数据链路层	根据帧物理地址进行网络间信息转发，可缓解网络通信繁忙度，提高效率。只能够连接相同 MAC 层的网络
路由器	网络层	通过逻辑地址进行网络间信息转发，可完成异构网络之间的互联互通，只能连接使用相同网络层协议的子网
网关	高层（4～7）	最复杂的网络互联设备，用于连接网络层上执行不同协议的子网（例如 Novell 与 SNA）
集线器	物理层	多端口中继器
二层交换机	数据链路层	指的是传统意义上的交换机，多端口网桥
三层交换机	网络层	带路由功能的二层交换机
多层交换机	高层（4～7）	带协议转换的交换机

3.3　局域网技术基础

局域网是一种在相对有限的地理范围内，通过一些网络设备将许多原本相对孤立的计算机资源（如 PC）及其他各种终端设备（如打印机）互联在一起，实现一个高速而稳定的数据传输和资源共享的计算机网络系统。

1．IEEE 802 参考结构

自 1980 年以来，许多国家和国际标准化机构都在积极进行局域网的标准化工作，其中最有影响力的是 IEEE 制定的局域网的 802 标准，包括 CSMA/CD、令牌总线和令牌环等，它被 ANSI 吸收为美国国家标准，被 ISO 作为国际标准。按照 IEEE 802 标准，局域网体系结构由物理层、媒体访问控制子层 MAC 和逻辑链路控制子层 LLC 组成，如图 3-8 所示。

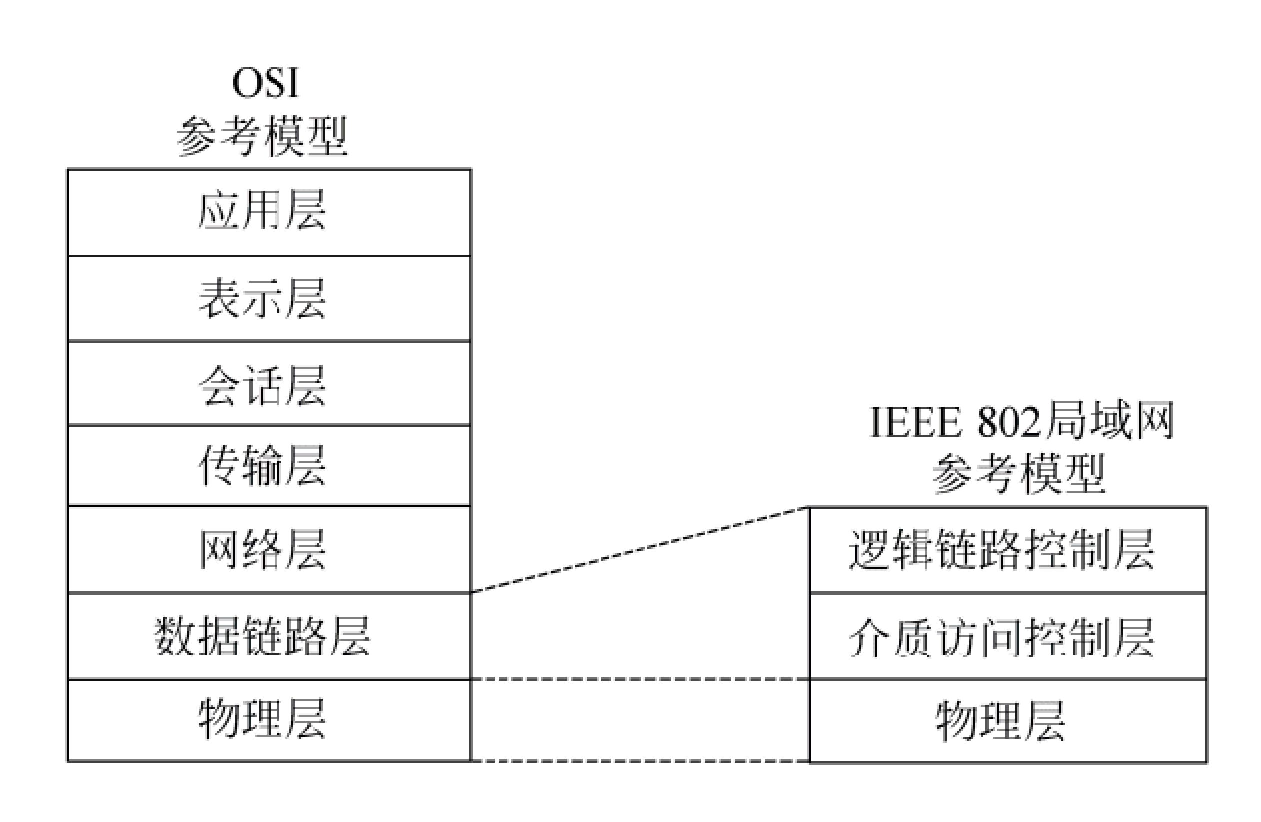


图 3-8　IEEE 802 标准的局域网参考模型与 OSI/RM 的对应关系

2．IEEE 802 标准

目前 IEEE 已经制定局域网标准有 10 多个，主要的标准如下：

IEEE 802.1 标准，定义了局域网标准概述、体系结构以及网络互联、网络管理等；

IEEE 802.2 标准，定义了逻辑链路控制 LLC 的功能与服务；

IEEE 802.3 标准，定义了带冲突检测的载波监听多路访问（Carrier Sense，Multiple Access with Collision Detection CSMA/CD）的总线介质访问控制方法和物理层规范；

IEEE 802.4 标准，定义了令牌总线（Token Bus）方式的介质访问控制方法和物理层规范；

IEEE 802.5 标准，定义了令牌环（Token Ring）方式的介质访问控制方法和物理层规范；

IEEE 802.6 标准，定义了城域网（MAN）介质访问控制方法和物理层规范；

IEEE 802.7 标准，定义了宽带技术；

IEEE 802.8 标准，定义了光纤技术；

IEEE 802.9 标准，定义了在 MAC 和物理层上的语音和数据综合局域网技术；

IEEE 802.10 标准，定义了可操作的局域网安全标准规范；

IEEE 802.11 标准，定义了无线局域网的 MAC 和物理层规范；

IEEE802.12 标准，定义了 100Mbps 高速以太网按需优先的介质访问控制协议 100VG-Any LAN；

IEEE 802.15 标准，定义了无线个人网 WPAN（Wireles Personal Area Network）；

IEEE 802.16 标准，定义了宽带无线访问标准。

3．局域网拓扑结构

计算机网络拓扑结构主要是指通信子网的物理拓扑结构。它通过网络中节点与通信线路之间的集合关系表示网络结构概况，反映出网络中各个实体间的结构关系。

1）总线型拓扑结构

总线型拓扑结构的最大特点就是结构简单，易于组网，而且只需要一条共享的通信线路，所以网络建设的成本相对比较低廉。当然总线型拓扑结构的网络也有一些缺点，如线路某一处损坏，能引起多个节点通信故障，也即就是我们通常所说的一点失效，会引起多点失效的现象；还有就是由于采用一条共享的通信线路，所以当网络系统负载比较大的情况下，所有的节点都会同时且不断地去竞争这条唯一的共享线路，导致系统的性能大幅下降。

总线拓扑结构是我们目前最常见的，也是最有代表性的。例如说我们现在使用最广泛的以太网（Ethernet）就是属于总线型拓扑结构。

2）环型拓扑结构

一个环型拓扑结构方式的网络，与总线形类似，也是由一条共享的通信线路把所有节点连接在一起，不过稍有不同的是，环型拓扑结构中的共享线路是闭合的，即它把所

有的站点最终排列成了一个环，每个站点只与其两个邻居直接相连。若一个站点想要给另一个发送信息，该报文必须经过它们之间的所有站点。

3）星型拓扑结构

一个星型拓扑结构方式的网络在直观上就很容易理解，就像是一张蜘蛛网，中间是一个枢纽（网络交换设备），所有的节点都被连接到这个枢纽上，最终组成一个星形的拓扑结构的网络。目前一般单位的局域网都是采用星型拓扑结构的网络，这当中我们熟悉的交换机就是处于中间枢纽位置上的网络交换设备。换言之，通过交换机（或集线器）来进行连接的网络都可以称为星型拓扑结构的网络。不过这里需要提醒大家注意的是：通过集线器来连接的这种网络只是在物理连线上属于星型拓扑结构，而在逻辑拓扑结构上来说，它仍然有可能是属于总线型拓扑结构的网络，因为网络中采取的媒体访问控制协议仍然可能是以太网协议（即 CSMA/CD 协议）。

4．局域网媒体访问控制技术

局域网媒体访问控制技术有多种方法，如总线型的以太网采用载波监听多路访问/冲突监测（CSMA/CD）介质访问控制方法，令牌环网采用令牌传送的控制方法等。

1）CSMA/CD 协议

IEEE 802.3 标准所采用的 CSMA/CD（载波监听多路访问/冲突检测）协议对于总线、星型和树型拓扑结构是最合适的介质访问控制协议，它属于竞争式介质访问控制协议。

CSMA/CD 的基本原理是：每个节点都共享网络传输信道，在每个站要发送数据之前，都会检测信道是否空闲，如果空闲则发送，否则就等待；在发送出信息后，则对冲突进行检测，当发现冲突时，则取消发送。

（1）载波监听。

冲突虽然没有办法避免，但是可以通过精心设计的监听算法来缓解，各种算法如表 3-9 所示。

表 3-9　载波监听算法

监 听 算 法	信道空闲时	信 道 忙 时	特　　点
非坚持型监听算法	立即发送	等待 N，再监听	减少冲突，信道利用率降低
1-坚持型监听算法	立即发送	继续监听	提高信道利用率，增大了冲突
P-坚持型监听算法	以概率 P 发送	继续监听	有效平衡，但复杂

注：非坚持型监听算法的 N 可取任意随机值，在 P-坚持型监听算法中，信道空闲将以概率（1–P）延迟一个时间单位（该时间单位为网络传输时延期τ）。

（2）冲突检测。

载波监听只能够减少冲突的概率，但无法完全避免冲突。为了能够高效地实现冲突检测，在 CSMA/CD 中采用了边发边听的冲突检测方法。也就是由发送者一边发，一边自己接收回来，如果发现结果一旦出现不同，马上停止发送，并发出冲突信号，这时所

有的站都会收到阻塞信息，并都等待一段时间之后再重新监听。而等待的这段时间的长度对网络的稳定工作有很大影响，常用的策略是“二进制指数后退算法”，算法如下：

对每个帧，当第一次发生冲突时，设置参量为 $L=2$；

退避间隔取 1～L 个时间片中的一个随机数，1 个时间片等于 $2a$（双向传播时间=$2a$，即：$a=0.5$）；

当帧重复一次冲突时，则将参量 L 加倍；

设置一个最大重传次数，超过这个次数，则不再重传，并报告出错。

而正是因为采用了边发边听的检测方法，因此检测冲突所需要花的最长时间是网络传播延迟的两倍（最大段长/信号传播速度，这是对于基带系统而言，有些宽带系统需要网络传播延迟的四倍时间才够），这称之为冲突窗口。因此，为了保证在信息发送完成之前能够检测到冲突，发送的时间应该大于等于冲突窗口，这也就规定了最小的帧长=2（网络数据速率×最大段长/信号传播速度）。

2）令牌环访问控制法

首先，令牌环网在网络中传递一个很小的帧，称为“令牌”，只有拥有令牌的工作站才有权力发送信息。

令牌在网络上依次序传递。

当工作站要发送数据时，等待捕获一个空令牌，然后将要发送的信息附加到后边，发往下一站，如此直到目标站。然后将令牌释放。

如果工作站要发送数据时，经过的令牌不是空的，则等待令牌释放。

从上面的介绍当中，令牌环访问控制法的缺点，就是协议过于复杂，所以造成了不必要的带宽开支，使得在低负载情况下令牌环网的速度比以太网慢得多。

5．以太网技术基础知识

以太网（Ethernet）最早是由 Xerox 公司在 20 世纪 70 年代提出的一个基带局域网标准。

在此基础上，IEEE 802 委员会的 802.3 工作组于 1983 年制定了第一个 IEEE 的以太网标准 IEEE 802.3，数据速率为 10Mbps。802.3 局域网对以太网标准中的帧格式作了一点很小的变动，但允许基于这两种技术的硬件实现在同一个局域网上互操作。

由于有关厂商在商业上的激烈竞争，IEEE 802 委员会制定了几个不同的局域网标准，例如 IEEE 802.4、IEEE 802.5 等等。直到 20 世纪 90 年代，激烈竞争的局域网市场初见明朗。以太网由于其成本低、灵活度高，相对简单、可靠性高以及数据传输率高等特点，成为应用最为广泛、最重要的局域网建设首选技术标准和最通用的通信协议标准。虽然其他网络新技术也曾经被认为很可能取代以太网的首选地位，但是仍然一直没有动摇和改变网络建设的技术设计人员对以太网的青睐。并且以太网也一直在不断地快速发展，不断地完善自己。

1）以太网技术基础

前面章节介绍以太网采用的是 CSMA/CD 媒体访问机制协议。另外以太网采用广播机制，所有与网络连接的工作站都可以收到其他站点发送到网络上的数据帧。每个工作站都要通过检测包含在数据帧中的目标地址字段来确认该数据帧是不是发送给自己的，如果已经确认数据帧是发给自己的，就将它交给高一层的协议层来处理。

2）以太网帧结构

以太网定义的帧结构和 IEEE 802.3 定义的帧结构是不同的，以太网帧的格式如图 3-9 所示，包含的字段有前导码（P）、目的地址（DA）、源地址（SA）、数据类型（TYPE）、发送的数据及帧校验序列（FCS）等。这些字段中除了数据字段是变长以外，其余字段的长度都是固定的。

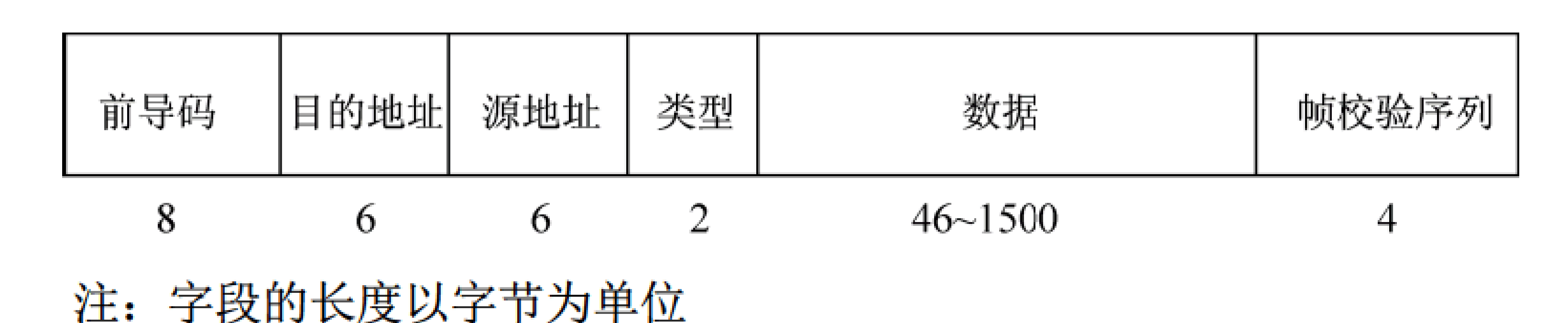


图 3-9　以太网的帧结构

3）IEEE 802.3 帧结构

IEEE 802.3 MAC 帧的格式如图 3-10 所示，包含的字段有前导码（P）、帧起始定界符（SFD）、目的地址（DA）、源地址（SA）、长度（LEN）、发送的数据及帧校验序列（FCS）等。这些字段中除了地址字段和数据字段是变长的以外，其余字段的长度都是固定的。

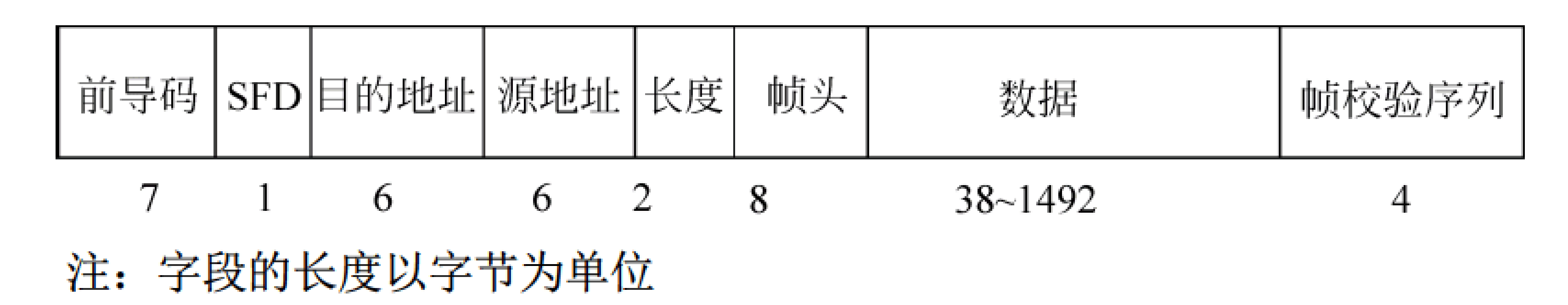


图 3-10　IEEE 802.3 MAC 帧的格式

4）以太网物理层规范

以太网比较常用的传输介质包括同轴电缆、双绞线、光纤三种，常以类似于 10Base-T 的形式来命名传输介质，如图 3-11 所示。

5）百兆、千兆、万兆交换型以太网

（1）百兆（快速）以太网。

随着计算机技术的不断发展，10Mbps 的网络传输速度实在无法满足日益增大的需求，人们就开始寻求更高的网络传输速度。但是由于 802.3 已被广泛应用于实际中，为了能够在它的基础上进行轻松升级，802.3u 充分考虑到了向下兼容性：它采用了非屏蔽双绞线（或屏蔽双绞线、光纤）作为传输介质，采用与 802.3 一样的介质访问控制层

——CSMA/CD。802.3u 常被称为快速以太网。

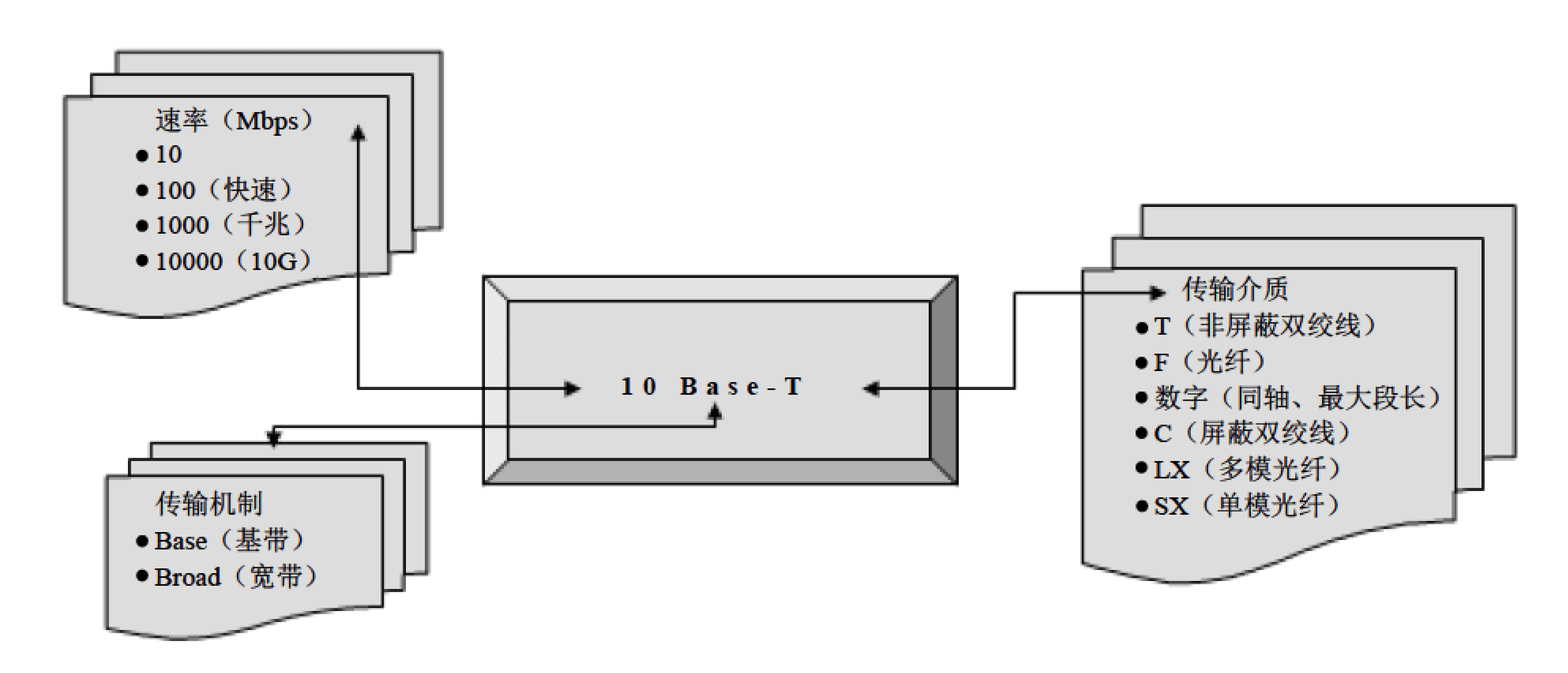


图 3-11 以太网传输介质标识

根据实现的介质不同，快速以太网可以分为 100Base-TX、100Base-FX 和 100Base-T4 三种。

（2）千兆以太网。

20 世纪 90 年代中期，随着各种新的网络技术的推出，仅有 100Mbps 传偷速度的以太网似乎已经发展到了极限，“以太网被淘汰了”的说法让以太网技术一度低靡。然而，1000Mbps 的千兆以太网的推出，给以太网技术注射了一针“强心针”，以太网技术迅速重新崛起。

802.3z 在 780nm 光纤上或超 5 类非屏蔽双绞线上运行。值得一提的是，为了给千兆以太网提供更好的传输介质，非屏蔽双绞线也推陈出新，不断地发展。首先是在 5 类双绞线的基础上进行改进，以适应千兆以太网的需要，接着又发展到了超 5 类和 6 类线。

（3）万兆以太网。

2002 年 6 月，IEEE 802.ae 10Gbps 以太网标准的发布，使得以太网的发展势头又得到了一次增强。确定万兆以太网标准的目的是将 IEEE 802.3 协议扩展到 10Gbps 的工作速度，并扩展以太网的应用空间，使之能够包括 WAN 链接。

6）全双工以太网

全双工以太网最大的特点是：交换设备工作时不同的逻辑数据通道之间已不再受到 CSMA/CD 的约束。全双工技术可以提供双倍于半双工操作的带宽，即每个方向都支持 10Mbps，这样就可以得到 20Mbps 的以太网带宽。当然这还与网络流量的对称度有关。

3.4 例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 8 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

基带同轴电缆的特性阻抗是__（1）__，CATV 电缆的特性阻抗是__（2）__。

（1）A．25Ω　　B．50Ω　　C．75Ω　　D．100Ω

（2）A．25Ω　　B．50Ω　　C．75Ω　　D．100Ω

例题 1 分析

同轴电缆以硬铜线为芯，外包一层绝缘材料。这层绝缘材料用密织的网状导体环绕，网外又覆盖一层保护性材料。有两种广泛使用的同轴电缆。一种是 50 欧姆电缆，用于数字传输，由于多用于基带传输，也叫基带同轴电缆；另一种是 75 欧姆电缆，公用天线电视系统（CATV）采用的标准电缆，它常用于传输频分多路 FDM 方式产生的模拟信号，频率可达 300～400MHz，称作宽带传输，也可用于传输数字信号。

例题 1 答案

（1）B　（2）C

例题 2

集线器是一种物理层联网设备，下面有关集线器的论述中，错误的是__（3）__。

（3）A. 集线器没有自动寻址能力

B. 连接在集线器上的故障设备不会影响其他节点通信

C. 集线器可以隔离广播风暴

D. 连接在集线器上的所有节点构成一个冲突域

例题 2 分析

“冲突域”是指会发生物理碰撞的域，可以通过加入第二层桥接技术或交换技术来进行逻辑分段，即可解决，也就是“用交换机/网桥解决介质争用问题”；但逻辑分段并没有分解了“广播域”，要分解广播域需要使用第三层设备（即路由器或三层交换机）。

（1）中继器、集线器（物理层）：单纯地放大，传播信号，运行在物理层。不能划分广播域也不能划分冲突域。

（2）网桥、二层交换机（数据链路层）：运行在数据链路层，可划分冲突域，不可划分广播域。

（3）路由器、网关、三层交换机、多层交换机（网络层及高层）：运行在网络层及高层以上，可划分冲突域，也可以划分广播域。

其中，前两项增加的冲突域的数量，减少了冲突域的范围；最后一项增加了广播域的数量，减少了广播域的范围，划分子网就属此类。

例题 2 答案

（3）C

例题 3

假设模拟信号的最高频率为 10MHz，采样频率必须大于__（4）__，得到的样本信号才能不失真。

（4）A. 5MHz　　B. 10MHz　　C. 15MHz　　D. 20MHz

例题 3 分析

最常用的编码技术是脉冲编码调制技术（PCM），简称为脉码调制。关于 PCM 原理中有以下几个关键知识点：

（1）PCM 要经过取样、量化、编码三个步骤。

（2）根据尼奎斯特取样定理，采样速率应大于模拟信号的最高频率的 2 倍。我们都知道 44kHz 的音乐让人感觉到最保真，这是因为人耳可识别的最高频率约为 22kHz，因此当采样率达到 44kHz 就可以得到最满意的效果。

（3）量化是将样本的连续值转成离散值，采用的方法类似于求圆周长时，用内切正多边形的方法。而平时，我们说 8 位、16 位的声音，指的就是 2^8、2^{16} 位量化。

（4）编码就是将量化后的样本值变成相应的二进制代码。

因此，要得到的样本信号不失真，需保证采样频率大于最高频率的两倍，即 20MHz。

例题 3 答案

（4）D

例题 4

设信道带宽为 4000Hz，调制为 4 种不同的码元，根据 Nyquist 定理，理想信道的数据速率为＿（5）＿。

（5）A. 4Kbps　　B. 8Kbps　　C. 16Kbps　　D. 24Kbps

例题 4 分析

根据奈奎斯特定理及码元速率与数据速率间的关系，数据速率 $R=2W\times \text{Log2}(N)$，可列出如下算式：

$R=2\times 4000\times \text{Log2}(4)=16\,000\text{bps}=16\text{Kbps}$

例题 4 答案

（5）C

例题 5

以下关于曼彻斯特编码的描述中，错误的是＿（6）＿。

（6）A. 无需另外传输同步信号

B. 每个比特都由两个码元组成

C. 用电平跳变来区分 0 和 1

D. 用电平的高低来区分 0 和 1

例题 5 分析

在曼彻斯特编码中，每一位的中间有一跳变，位中间的跳变既作时钟信号，又作数据信号；通常从高到低跳变表示“1”，从低到高跳变表示“0”（其中反过来描述也是正确的）。

例题 5 答案

（6）D

例题 6

一个 8 口的 10Base-T 集线器，每个端口的平均带宽是__（7）__。一个 8 口的 10Base-T 交换机，一个端口通信的数据速率（半双工）最大可以达到__（8）__。

（7）A. 10Mbps　　B. 8Mbps　　C. 2Mbps　　D. 1.25Mbps

（8）A. 10Mbps　　B. 8Mbps　　C. 2Mbps　　D. 1.25Mbps

例题 6 分析

集线器属于共享带宽网络设备，在半双工状态下工作。

它的端口带宽＝背板带宽（集线器）/端口数量

交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。

例题 6 答案

（7）D　　（8）A

例题 7

因特网中的协议应该满足规定的层次关系，下面的选项中能正确表示协议层次和对应关系的是__（9）__。

（9）A.

TFTP	Telnet
UDP	TCP
IP	

B.

RIP	Telnet
TCP	ARP
IP	

C.

HTTP	SNMP
UDP	UDP
IP	

D.

SMTP	FTP
TCP	UDP
IP	

例题 7 分析

传输层基于 TCP 协议的应用层协议有：FTP（文件传输协议）、TELNET（远程登录协议）、HTTP（超文本传输协议）、SMTP（简单邮件传输协议）。

传输层基于 UDP 协议的应用层协议有：TFTP（简单文件传输协议）、SNMP（简单网络管理协议）、HTTPS（安全 HTTP 协议）、DHCP（动态主机控制协议）。

例题 7 答案

（9）A

例题 8

下面关于 ARP 协议的描述中，正确的是__（10）__。

（10）A. ARP 报文封装在 IP 数据报中传送

B. ARP 协议实现域名到 IP 地址的转换

C. ARP 根据 IP 地址获取对应 MAC 地址

D. ARP 协议是一种路由协议

例题 8 分析

ARP（Address Resolution Protocol，地址解析协议）是一个位于 TCP/IP 协议栈中的低层协议，负责将某个 IP 地址解析成对应的 MAC 地址。

当一个基于 TCP/IP 的应用程序需要从一台主机发送数据给另一台主机时，它把信息分割并封装成包，附上目的主机的 IP 地址。然后，寻找 IP 地址到实际 MAC 地址的映射，这需要发送 ARP 广播消息。当 ARP 找到了目的主机 MAC 地址后，就可以形成待发送帧的完整以太网帧头。最后，协议栈将 IP 包封装到以太网帧中进行传送。

例题 8 答案

（10）B

第 4 章 计算机网络应用基础

根据考试大纲的要求，本章需要考生掌握的内容主要有三大板块：因特网应用基础、网络操作系统基础和应用服务器基础。

4.1 因特网基础知识

本节考查知识主要包括因特网的概念、起源和提供的一些基本服务。

4.1.1 因特网简介

因特网起源于20世纪70年代美国国防部高级计划研究局DARPA（Defense Advanced Research Project Agency）为应对冷战时代核战争的需要，当网络的某一部分因遭受攻击而失去工作能力时，网络的其他部分应当能够维持正常通信。

1969 年 DARPA 建立了一个覆盖全国的著名网络 ARPANET（Advanced Research Project Agency Network），其采用分组交换技术，使用报文处理机 IMP（Interface Message Processors）实现网络互联，最基本的服务是资源共享，互换信息，可实现异地的电子会议和网上的文件传输。

ARPANET 的成功极大地促进了网络互联技术的发展，于 1979 年完成了传输控制协议/互联网络协议（即 TCP/IP）规范，1980 年开始在 ARPANET 全面推广，1983 年完成。1986 年美国国家科学基金会 NSF（National Science Foundation）采用 TCP/IP 通信协议建立起 NSFNET 网络，且与 ARPANET 相连，并逐渐取代了 ARPANET 网络，形成了因特网的雏形。1988 年后，NSFNET 由全美国 13 个节点为主干节点，成为因特网的主干网，此后各国也相继建立了本国的 TCP/IP 网络，并连接到美国的因特网，逐步形成了覆盖全世界的因特网。

1．因特网的概念

因特网是一个全球范围的计算机网络，它把全世界数以百万计的计算机设备互连在一起。这些计算设备大多数是传统的台式 PC、Unix 工作站，以及存储并传输诸如 Web 页面和电子邮件消息等信息的所谓服务器。诸如 Web TV、笔记本、传呼机等等非传统的计算设备也越来越多的连接到因特网当中。因特网以相互交流信息资源为目的，基于一些共同的协议，由许多路由器和公共互联网组成，它是一个信息资源和资源共享的集合。

2．因特网提供的基本服务

因特网是一个庞大的互联系统，其上的巨大资源是人类智慧的结晶，为了充分地使用这些丰富而宝贵的资源，因特网提供了种类繁多的网络服务。主要有：

1）电子邮件

电子邮件（Electronic Mail）亦称 E-mail。它是用户或用户组之间通过计算机网络收发信息的服务。目前电子邮件已成为网络用户之间快速、简便、可靠且成本低廉的现代通信手段，也是因特网上使用最广泛、最受欢迎的服务之一。

2）文件传输

因特网的入网用户可以利用“文件传输服务（FTP）”命令系统进行计算机之间的文件传输，使用 FTP 几乎可以传送任何类型的多媒体文件，如图像、声音、数据压缩文件等。

3）远程登录

远程登录（Telnet）是 Internet 提供的最基本的信息服务之一，远程登录是在网络通信协议 Telnet 的支持下使本地计算机暂时成为远程计算机仿真终端的过程。在远程计算机上登录，必须事先成为该计算机系统的合法用户并拥有相应的账号和口令。登录时要给出远程计算机的域名或 IP 地址，并按照系统提示，输入用户名及口令。登录成功后，用户便可以实时使用该系统对外开放的功能和资源。

4）网络视频会议

网络视频会议技术是一种基于 IP 技术、流媒体技术在互联网上进行的一种全新通信方式，它不仅有传统视频和电话会议的图像和声音交流，而且能提供各种文档、软件，甚至远程计算机之间的交流功能。用户不需要购买终端设备，也不需要租用专线，只要有一台能上网的计算机，就可以不受时间、地点的限制，与任何人实现“面对面”地交流和“手把手”地工作。它能够提供图像、声音、文档、应用程序、网页、桌面、流媒体等多项共享功能，除了通常意义上的会议用途外，还可以用来开展教学和培训，组织网上销售和市场推广活动，进行售前或售后培训、远程客户维护、协同工作等。

5）电子商务

电子商务就是指贸易活动各环节的电子化，它覆盖与商务活动有关的所有方面。按照世界贸易组织的定义，电子商务就是通过电信网络进行的生产、营销、销售与流通活动，不仅指基于 Internet 的交易，而且指所有利用电子信息技术来解决扩大宣传、降低成本、增加价值和创造商机的商务活动，它包括通过网络实现从原材料查询、采购、产品展示、订购的生产、储运及电子支付等一系列的贸易活动。

电子商务主要覆盖三方面的内容：一是政府贸易管理的电子化，即采用网络技术实现数据和资料的处理、传递和存储；二是企业级电子商务，即企业间利用计算机技术和网络技术实现供货商、用户之间的商务活动；三是电子购物，即企业通过网络为个人提供的电子支付形式的服务及商业行为。

电子商务按照其交易对象分为 B2B（Business to Business）、B2C（Business to Citizen）、C2C（Citizen to Citizen）三类。其中 B2B 代表商家对商家，B2C 代表商家对个人，C2C 代表个人对个人。

6）电子政务

电子政务是指政府机构利用信息化手段，实现各类政府职能。其核心是：应用信息技术，提高政府事务处理的信息流效率，改善政府组织和公共管理。

电子政务的应用模式分为 G2G（Government to Government）、G2B（Government to Business）、G2C（Government to Gitizen）三类，其中 G2G 代表不同的政府机构对不同的政府机构，G2B 代表政府机构对商家或企业，G2C 代表政府机构对公民。

4.1.2　WWW 基础概念

WWW 是因特网的最主要应用之一，它使用超文本和超媒体技术，为用户提供了一种连机交互查询信息的方式。WWW 中的几个重要概念介绍如下。

1．超文本标记语言

超文本标记语言（Hyper Text Markup Language，HTML）是一种特定类型的超文本，是一种专门的编程语言，用于 Web 上，创建存储在 WWW 服务器上的文件。它是所有的因特网站点共同的语言，所有的网页都是以 HTML 格式的文件为基础，再加上一些其他语言工具（例如 JavaScript、VBScript、Java Applet 等）构成的。

2．统一资源定位器

统一资源定位器（Unifrom Resource Locator，URL）是 WWW 上的一种编址机制，用于对 WWW 的资源进行定位，以便于检索和浏览。

URL 由三部分组成：其一是它所使用的因特网文档传送协议，其二是标识要检索的主机代号（域名），其三是检索文档所在主机的路径及文件名。

3．主页

主页是一个 Web 站点的首页，是进入一个站点首先看到的页，它包含了连接到同一站点其他页面的超级链接，也包含了到其他站点的超级链接。建立主页对于企业来说可以树立企业形象、扩大市场范围、为客户提供信息查询，建立主页的首要条件是在因特网上有一块属于自己的存储空间，用于存放主页，通常获得这个空间有三种方式：建立自己的 WWW 服务器并申请接入到因特网上、租用因特网服务商的虚拟主机和申请免费空间。

4．浏览器

WWW 浏览器是用于观看万维网（WWW）信息的可独立运行的用户应用程序，通过这些程序，用户可以访问因特网上的任何站点，并观看其上的超文本信息。

WWW 浏览器程序很多，主要的有 IE、Google Chrome、Firefox、Opera 等。目前使用最多的是微软的 IE 浏览器。

4.2 网络操作系统

从资源管理的观点，网络操作系统（NOS）是向网络计算机提供网络通信和网络资源共享功能，负责管理整个网络资源和方便网络用户使用的程序集合。

4.2.1 网络操作系统简介

网络操作系统是网络的心脏和灵魂。它运行在服务器上，所以有时我们也把它称之为服务器操作系统。

1．网络操作系统的功能

网络操作系统的基本功能就是要管理网络系统的软硬件资源，实现网络范围的资源共享。为了实现上述功能，计算机网络的另一个重要任务就是数据通信。于是，网络操作系统除了具备通常（单机）操作系统所具备的功能外，还应具有网络支持功能，包括通信服务和网络的控制等功能。

网络操作系统的主要功能有：

（1）具有通常操作系统的所有功能：即处理机管理、存储器管理、作业管理、设备管理、文件管理等功能。

（2）网络通信功能：通过网络协议进行高效、可靠的数据传输和具有很强的网络通信能力。除了支持终端与主机之间的通信外，还要具有主机与主机之间的通信以及多个"用户对"之间同时通信的能力，即将一条物理链路虚拟为多条逻辑链路的功能。在出现异常事件时，还应具有及时进行处理的能力。

（3）网络资源管理功能：它协调各用户对网络硬软件资源的使用。

（4）提供各种网络服务功能。

（5）网络管理功能：网络管理包括安全管理、故障管理、性能管理等。

2．网络操作系统的结构

一些自主的计算机系统，可通过通信设施相互联接，完成信息交换、资源共享、互操作和协同工作等功能。引入计算机网络的目的是要完成新的应用，进行自动的信息交换，以及共享昂贵的硬软件资源，提高性价比。网络功能与通常操作系统的结合程度是网络操作系统的重要性能指标。早期的做法是采用在通常操作系统的基础上附加网络软件，并使网络功能成为操作系统的有机组成部分的结构。

随着互联网的发展，网络规模和复杂程度的增大，早期的结构难以适应复杂的网络操作系统的要求。从网络安全角度，也要求把系统内核中可能引起安全性问题的部分内容删除出去。因此需要重新按计算机网络系统的要求来重新构造网络操作系统。目前存在着多种网络操作系统并存的情况，不同网络操作系统的结构也不相同。比较常用的是采用客户/服务器模型的结构。

3．常见的网络操作系统

网络操作系统是组建网络的关键因素之一，Windows、UNIX 和 Linux 是目前使用最为流行的几个网络操作系统。

1）Windows 类网络操作系统

微软公司的 Windows 系统不仅在个人操作系统中占有绝对优势，它在网络操作系统中也是具有非常强劲的力量。在局域网中，微软的网络操作系统主要有：Windows NT 4.0、Windows 2003 Server/Advance Server，以及最新的 Windows Server 2008 / Advance Server 等。

希赛教育专家特别提示：Windows 部分需要掌握系统的安装，配置以及基本应用，由于 Windows 类操作系统比较普及，本书不再重点介绍。

2）UNIX 网络操作系统

UNIX 是最早推出的网络操作系统。UNIX 是一个通用的、多用户的计算机分时系统，并且是大型机、中型机以及若干小型机上的主要操作系统，目前广泛地应用于教学、科研、工业和商业等多个领域。

UNIX 系统提供的服务与其他操作系统所提供的服务基本上一样。它为连接到大多数计算机上的各种各样的外部设备提供了方便和一致的接口；为信息管理提供文件系统。它支持网络文件系统服务，提供数据等应用，功能强大，系统稳定和安全性能比较好。

UNIX 最主要的长处之一是其可移植性强，它可以在各种不同类型的计算机上运行。在 UNIX 系统的控制下，某类计算机上运行的普通程序通常不作修改或作很少的修改就可以在别的类型的计算机上运行。另外分时操作也是 UNIX 的一个十分重要的特点，UNIX 系统把计算机的时间分成若干个小的等份，并且在各个用户之间分配这些时间。

UNIX 开创了许多重要的概念。其中最重要的当属管道（Pipe）概念，由管道概念导致了这样的思想：复杂的功能可以通过编制成一组在一起工作的程序来实现。

3）Linux 网络操作系统

Linux 操作系统最大的特点就是源代码开放，可以免费得到许多应用程序。目前也有中文版本的 Linux，如 RedHat（红帽子）、红旗 Linux 等等，都得到了用户充分的肯定。Linux 的优点主要体现在它的安全性和稳定性方面。它与 UNIX 操作系统有许多类似之处。

对于不同的网络应用，需要我们有目的有选择地使用合适的网络操作系统。

希赛教育专家特别提示：Linux 部分需要掌握系统的安装，配置以及 Linux 操作命令。下面就来重点介绍 Linux 操作系统。

4.2.2　Linux 操作系统

Linux 是芬兰赫尔辛基大学的学生 Linus Torvalds 设计开发的，后来经过众多世界顶尖的软件工程师的不断修改和完善，Linux 得以在全球普及开来，在服务器领域及个人桌面版得到越来越多的应用，在嵌入式开发方面更是具有其他操作系统无可比拟的优势，

目前每年用户递增数量体现了 Linux 强大的力量。

1．Linux 操作系统的构成

Linux 一般有四个主要部分构成：内核、Shell、文件结构和实用工具。

1）内核

内核作为 Linux 操作系统的心脏，是运行程序和管理像磁盘和打印机等硬件设备的核心程序。

2）Linux Shell

Shell 是系统的用户界面，提供了用户与内核进行交互操作的一种接口。它接收用户输入的命令并把它送入内核去执行。

实际上 Shell 是一个命令解释器，它解释由用户输入的命令并且把它们送到内核。不仅如此，Shell 有自己的编程语言用于对命令的编辑，它允许用户编写由 Shell 命令组成的程序。Shell 编程语言具有普通编程语言的很多特点，比如它也有循环结构和分支控制结构等，用这种编程语言编写的 Shell 程序与其他应用程序具有同样的效果。

Linux 提供了像 Microsoft Windows 那样的可视的命令输入界面——X Window 的图形用户界面（GUI）。它提供了很多窗口管理器，其操作就像 Windows 一样，有窗口、图标和菜单，所有的管理都是通过鼠标控制。现在比较流行的窗口管理器是 KDE 和 GNOME。

每个 Linux 系统的用户可以拥有他自己的用户界面或 Shell，用以满足他们自己专门的 Shell 需要。

3）Linux 文件结构

文件结构是文件存放在磁盘等存储设备上的组织方法。主要体现在对文件和目录的组织上。目录提供了管理文件的一个方便而有效的途径。我们能够从一个目录切换到另一个目录，而且可以设置目录和文件的权限，设置文件的共享程度。

使用 Linux，用户可以设置目录和文件的权限，以便允许或拒绝其他人对其进行访问。Linux 目录采用多级树型结构。用户可以浏览整个系统，可以进入任何一个已授权进入的目录，访问那里的文件。

文件结构的相互关联性使共享数据变得容易，几个用户可以访问同一个文件。Linux 是一个多用户系统，操作系统本身的驻留程序存放在以根目录开始的专用目录中，有时被指定为系统目录。

内核，Shell 和文件结构一起形成了基本的操作系统结构。它们使得用户可以运行程序，管理文件以及使用系统。此外，Linux 操作系统还有许多被称为实用工具的程序，辅助用户完成一些特定的任务。

4）Linux 实用工具

标准的 Linux 系统都有一套叫做实用工具的程序，它们是专门的程序，例如编辑器、执行标准的计算操作等。用户也可以产生自己的工具。

实用工具可分三类：

- 编辑器：用于编辑文件。
- 过滤器：用于接收数据并过滤数据。
- 交互程序：允许用户发送信息或接收来自其他用户的信息。

Linux 的编辑器主要有 Ed、Ex、Vi 和 Emacs。Ed 和 Ex 是行编辑器，Vi 和 Emacs 是全屏幕编辑器。

Linux 的过滤器（Filter）读取从用户文件或其他地方的输入，检查和处理数据，然后输出结果。从这个意义上说，它们过滤了经过它们的数据。Linux 有不同类型的过滤器，一些过滤器用行编辑命令输出一个被编辑的文件。另外一些过滤器是按模式寻找文件并以这种模式输出部分数据。还有一些执行字处理操作，检测一个文件中的格式，输出一个格式化的文件。过滤器的输入可以是一个文件，也可以是用户从键盘键入的数据，还可以是另一个过滤器的输出。过滤器可以相互联接，因此一个过滤器的输出可能是另一个过滤器的输入。在有些情况下，用户可以编写自己的过滤器程序。

交互程序是用户与机器的信息接口。Linux 是一个多用户系统，它必须和所有用户保持联系。信息可以由系统上的不同用户发送或接收。信息的发送有两种方式，一种方式是与其他用户一对一地链接进行对话，另一种是一个用户对多个用户同时链接进行通信，即所谓广播式通信。

2．文件与目录操作

用户的数据和程序大多以文件的形式保存。用户使用 Linux 系统的过程中，需要经常对文件和目录进行操作，文件和目录操作是 Linux 的基础。

1）文件与文件名

在多数操作系统中都有文件的概念。文件是 Linux 用来存储信息的基本结构，它是以文件名来命名并存储在某种介质（如磁盘、光盘和磁带等）上的一组信息的集合。Linux 文件均为字符流形式。文件名是文件的标识，它由字母、数字、下划线和圆点组成的字符串来构成。用户应该选择有意义的文件名。Linux 要求文件名的长度限制在 255 个字符以内。

为了便于管理和识别，用户可以把扩展名作为文件名的一部分。圆点用于区分文件名和扩展名。扩展名对于将文件分类是十分有用的。用户可能对某些大众已接纳的标准扩展名比较熟悉，例如，C 语言编写的源代码文件总是具有 C 的扩展名。用户可以根据自己的需要，随意加入自己的文件扩展名。

2）文件的类型

Linux 文件系统包括：文本文件、二进制文件、目录文件、连接文件、设备文件、管道文件（用于进程间通信）。网络管理员考试主要考设备文件相关知识。其中设备文件是 Linux 系统很重要的一个特色。Linux 系统把每一个 I/O 设备都看成一个文件，与普通文件一样处理，这样可以使文件与设备的操作尽可能统一。从用户的角度来看，对 I/O 设备的使用和一般文件的使用一样，不必了解 I/O 设备的细节。设备文件可以细分为块

设备文件和字符设备文件。前者的存取是以一个个字符块为单位的，后者则是以单个字符为单位的。

3）目录

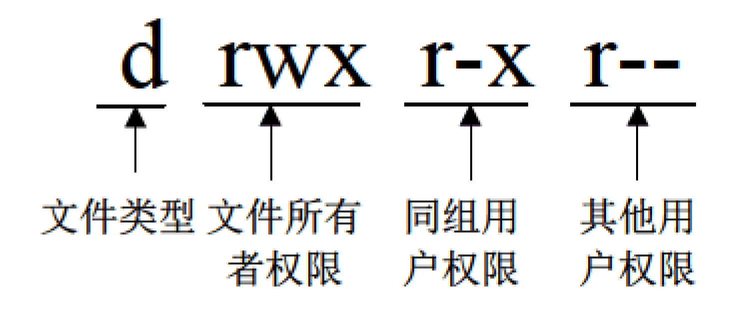
Linux 系统以文件目录的方式来组织和管理系统中的所有文件。所谓文件目录就是将所有文件的说明信息采用树型结构组织起来，即我们常说的目录。也就是说，整个文件系统有一个“根”（root），然后在根上分“杈”（directory），任何一个分杈上都可以再分杈，杈上也可以长出“叶子”。“根”和“杈”在 Linux 中被称为是“目录”或“文件夹”。而“叶子”则是一个个的文件。目录也是一种类型的文件。Linux 系统通过目录将系统中所有的文件分级、分层组织在一起，形成了 Linux 文件系统的树型层次结构。以根目录为起点，所有其他的目录都由根目录派生而来。实践证明，此种树型结构的文件系统效率比较高。

4）用户权限

Linux 下有两种用户：

- root 用户：超级权限者，系统的拥有者，在 Linux 系统中有且只有一个 root 用户，它可以在系统中进行任何操作。在系统安装时所设定的密码就是 root 用户的密码。
- 普通用户：Linux 系统可以创建许多普通用户，并为其指定相应的权限，使其有限地使用 Linux 系统。

在 Linux 系统中，每一个文件和目录都有相应的访问许可权限，文件或目录的访问权限分为可读（可列目录）、可写（对目录而言是可在目录中做写操作）和可执行（对目录而言是可以访问）三种，分别以 r，w，x 表示，其含义为：对于一个文件来说，可以将用户分成文件所有者、同组用户、其他用户三种类型，每种用户都被赋予了不同的权限。每一个文件或目录的访问权限都有三组，每组用三位表示，如图 4-1 所示。



注：文件类型有多种，d 代表目录，-代表普通文件，c 代表字符设备文件。

图 4-1 权限位示意图

改变权限 chmod 命令的语法格式为：chmod[who][opt][mode]文件/目录名。

其中 who 表示对象，是以下字母中的一个或组合：u（文件所有者）、g（同组用户）、o（其他用户）、a（所有用户）；opt 则是代表操作，可以为：+（添加权限）、—（取消权限）、=（赋予给定的权限，并取消原有的权限）；而 mode 则代表权限。有时候也常用字表示法来表示权限，即读取（r），写入（w）和执行（x）分别以 4、2、1 来代表，没有授予的部分就表示值为 0。

3．系统基本操作命令

Linux 可以通过命令的方式来管理操作系统，其命令可以完成很多复杂的工作。Linux 一些常用的命令如表 4-1 所示。

表 4-1　Linux 常用命令

命　令	命 令 说 明	等价的 DOS 命令
pwd	显示当前工作目录和路径名	不带参数的 cd 命令
ls	列出目录内容	dir 命令
cp	复制文件内容，可复制整个目录	copy 命令
cat	串接并显示文件，可同时显示多个文件	type 命令
cd	改变当前工作目录	cd 命令
rm	删除文件和目录	del 和 rmdir 命令
mv	移动文件	move 命令
ps	显示当前进程	无对应
kill	中止某个进程	无对应
chmod	设置文件、目录的权限	无对应

另外，还有几个命令在往年考试中也有考查，具体介绍如下：

（1）Tar 命令。

格式：tar 选项文件目录列表。

功能：对文件目录进行打包备份。

选项：

-c，建立新的归档文件；

-r，向归档文件末尾追加文件；

-x，从归档文件中解出文件；

-O，将文件解开到标准输出；

-v，处理过程中输出相关信息；

-f，对普通文件操作；

-z，调用 gzip 来压缩归档文件，与-x 联用时调用 gzip 完成解压缩；

-Z，调用 compress 来压缩归档文件，与-x 联用时调用 compress 完成解压缩。

例如，将当前目录下所有.txt 文件打包并压缩归档到文件 this.tar.gz，可以使用：

tar czvf this.tar.gz./*.txt

将当前目录下的 this.tar.gz 中的文件解压到当前目录可以使用：

tar xzvf this.tar.gz./

（2）cd 命令。

格式：cd [dirName]

功能：变换工作目录至 dirName。其中 dirName 表示法可为绝对路径或相对路径。

若目录名称省略，则变换至使用者的 home directory（也就是刚 login 时所在的目录）。另外，“~”也表示为 home directory 的意思，“.”则是表示目前所在的目录，“..”则表示目前目录位置的上一层目录。

例如：

跳到 /usr/bin/：cd /usr/bin

跳到自己的 home directory：cd ~

跳到目前目录的上上两层：cd ../..

返回进入当前目录前所在目录：cd -

4.3 应用服务器基础知识

根据对考试大纲的解读，希赛教育专家特别提示，本节要求考生主要掌握的内容有：DNS 服务的基本原理、WWW 服务的基本原理、FTP 服务的基本原理、电子邮件服务的基本原理、DHCP 服务器的基本原理以及代理服务器的基本原理。

4.3.1 DNS 服务的基本原理

DNS 服务是 Internet 上最常见的服务之一，它是现在网络系统中不可或缺的组成部分。

1．域名系统 DNS 概述

IP 地址符合了对地址唯一性的需要，Internet 上的每一台主机都被分配了一个独立的 IP 地址，但由于 IP 地址是用 32 位的数字组成，人们记忆起来比较困难，域名就应运而生。域名系统 DNS 是因特网使用的命名系统，它的功能是用于实现主机名与主机地址之间的映射。

2．域名系统 DNS 解析原理

从理论上讲，整个因特网可以只使用一个域名服务器，使它装入因特网上所有的主机名，并回答所有对 IP 地址的查询。然而这种做法并不可取。因为因特网规模很大，这样的一个域名服务器肯定会因为负荷而无法正常工作，而且一旦域名服务器出现故障，整个因特网就会瘫痪。因此，早在 1983 年因特网就开始采用层次树状结构的命名方法，并使用分布式的域名系统 DNS。

因特网的域名系统 DNS 被设计成为一个联机分布式数据库系统，并采用客户/服务器模式。域名到 IP 地址的解析过程如下：大多数名字都在本地进行解析，当某一个应用进程需要把主机名解析为 IP 地址时，该应用进程就调用解析程序，并成为 DNS 的一个客户，把待解析的域名放在 DNS 请求报文中，以 UDP 用户数据报方式发给本地域名服务器。本地域名服务器在查找域名后，把对应的 IP 地址放在回答报文中返回。应用进程获得目的主机的 IP 地址后即可进行通信。

4.3.2　WWW 服务的基本原理

WWW 服务也是目前 Internet 上应用最为广泛的服务之一。下面来具体分析一下 WWW 服务的体系结构与工作过程。

1．WWW 服务体系结构

WWW 采用了浏览器/服务器模型，用户使用本地计算机运行 WWW 的客户程序（如 IE），用户将要访问服务器，则运行 WWW 服务程序。用户通过 WWW 客户程序向 WWW 服务器发出一个查询请求，WWW 服务器接收到此请求，并将在本服务器内检索到的对应内容返回给用户。

2．WWW 服务工作过程

WWW 的工作过程可以简单归纳如下：

（1）客户端启动 Web 客户程序，通常是 IE 浏览器。

（2）如果客户端程序配置了默认主页连接，则自动连接到主页上，否则它只是启动，等待输入。

（3）在客户端程序输入想查看的 Web 页的地址（如http://www.educity.cn）。

（4）客户端程序与该地址的服务器连通，并告诉服务器需要哪一页。

（5）服务器将该页发送给客户程序。

（6）客户程序显示该页内容。

（7）用户可以阅读该页内容。

（8）每页还包含指向其他页的链接，有时还有指向本页其他内容的链接，用户只要单击该链接就可到达相应的地方。

4.3.3　FTP 服务的基本原理

文件传输协议 FTP 是因特网上使用得最为广泛的协议之一，提供交互式的访问，允许客户指明文件的类型与格式，并允许文件具有存取权限。FTP 屏蔽了各计算机系统的细节，因而适合于在异构网络中任意计算机之间传送文件，很早就成为了因特网的正式标准。

1．FTP 的基本工作原理

FTP 是基于客户/服务器（C/S）模型设计的，客户与服务器之间利用 TCP 建立连接，与一般客户/服务器模型不同的是，FTP 客户端与服务器之间要建立双重连接，一个是控制连接，一个是数据连接。建立双重连接的原因在于：FTP 是一个交互式会话系统，FTP 客户进程每次调用 FTP 便于服务器建立一个会话，会话以控制连接来维护，直至退出 FTP。

控制连接负责传输控制信息，尤其是客户命令（如文件传输命令），FTP 客户每提出一个请求，服务器便与客户建立一个数据连接，进行实际的数据传输。数据传输完毕

后，数据连接就被撤销，但控制连接依然存在，客户可以继续发出命令，直到客户输入撤销命令撤销控制连接。为了满足多个 FTP 客户进程的请求需要，FTP 服务器采用并发服务器方式。

2．匿名 FTP

为了保证安全性，用户在访问 FTP 服务器上传/下载文件之前必须首先进行登录，需要输入在 FTP 服务器上合法的用户名和口令，只有登录成功后才对文件进行列表、上传及下载服务。为了便于一些公共资料的传播，许多 FTP 服务器提供了匿名 FTP 服务，便于大家的上传下载。

匿名 FTP 服务的含义是，在提供 FTP 服务的服务器上建立一个公开的账户（通常为 anonymous），并授予该账户访问公共目录和下载指定公共文件的权限。用户访问这些 FTP 服务器，一般不需要输入用户名和密码，如果需要输入的话，用户名和密码通常分别为 anonymous 和用户自己的电子邮件地址。为了保证 FTP 服务器的安全性，一般的匿名 FTP 服务都只给用户提供下载权限，而不提供上传权限。

4.3.4 电子邮件的基本原理

电子邮件是因特网上应用范围最为广泛的服务，它是通过计算机网络与其他用户进行联络的快速、安全、高效、价廉的现代化通信手段。

1．电子邮件的基本工作原理

电子邮件（E-mail）是一种利用网络交换信息的非交互式服务。邮件服务器是电子邮件系统的核心，一份电子邮件一般涉及两个邮件服务器，发送方服务器和接收方服务器。发送方服务器的功能是依照收件人地址将邮件发送出去，发送方服务器就像普通的发信邮局；接收方服务器的功能是接收他人的来信并且把它保存，随时供收件人阅读，就像普通收信的邮局。电子邮件模仿传统的邮政业务，通过建立邮政中心，在中心服务器上给用户分配电子信箱，也就是在服务器硬盘上划出一块区域，相当于邮局，在这块存储区内又分成许多小区，就是每个用户的电子信箱。使用电子邮件的用户都可以通过各自的计算机或终端编辑信件，通过 Internet 送到对方的信箱中，对方用户进入电子邮件系统就可以读取自己信箱中的信件，邮件才从服务器的硬盘转存到本地计算机的硬盘中。

如要使用电子邮件服务，首先需要一个电子邮箱，电子邮箱通常由电子邮件服务提供商（如 ISP）提供，当用户向 ISP 申请电子邮箱时，ISP 会在电子邮件服务器上建立一个电子邮件账号，包括用户名和密码，任何人都可以将邮件发送到此电子邮箱中，但只有输入正确的用户名和密码，用户才可以看到电子邮件内容。

每个电子邮箱都有一个邮箱地址，称为电子邮件地址，其格式为：用户名@主机名，如 master@csai.cn，master 是用户名，mail.csai.cn 是电子邮件服务器的主机地址。

2．电子邮件的应用程序

通过使用本地计算机的电子邮件应用程序才能发送和接收电子邮件，目前电子邮件

应用程序很多，最常用的是 Outlook Express 和 Foxmail。在电子邮件应用程序向电子邮件服务器发送邮件时使用的是 SMTP 协议（Simple Mail Transfer Protocol，简单邮件传输协议），电子邮件应用程序从电子邮件服务器接收邮件时，使用的通常是 POP3 协议（Post Office Protocol，邮局协议）或 IMAP 协议（Ineteractive Mail Access Protocol，交互式邮件存取协议）。

4.3.5　DHCP 服务的基本原理

在一个使用 TCP/IP 协议的网络中，每一台计算机都必须至少有一个 IP 地址，才能与其他计算机连接通信。为了便于统一规划和管理网络中的 IP 地址，DHCP 动态主机配置协议应运而生了。这种网络服务有利于对局域网中的客户机 IP 地址进行有效管理，而不需要一个一个手动指定 IP 地址。

DHCP 工作原理如下：

DHCP 是基于客户机/服务器模型设计的，DHCP 客户和 DHCP 服务器之间通过收发 DHCP 消息进行通信，如图 4-2 所示。

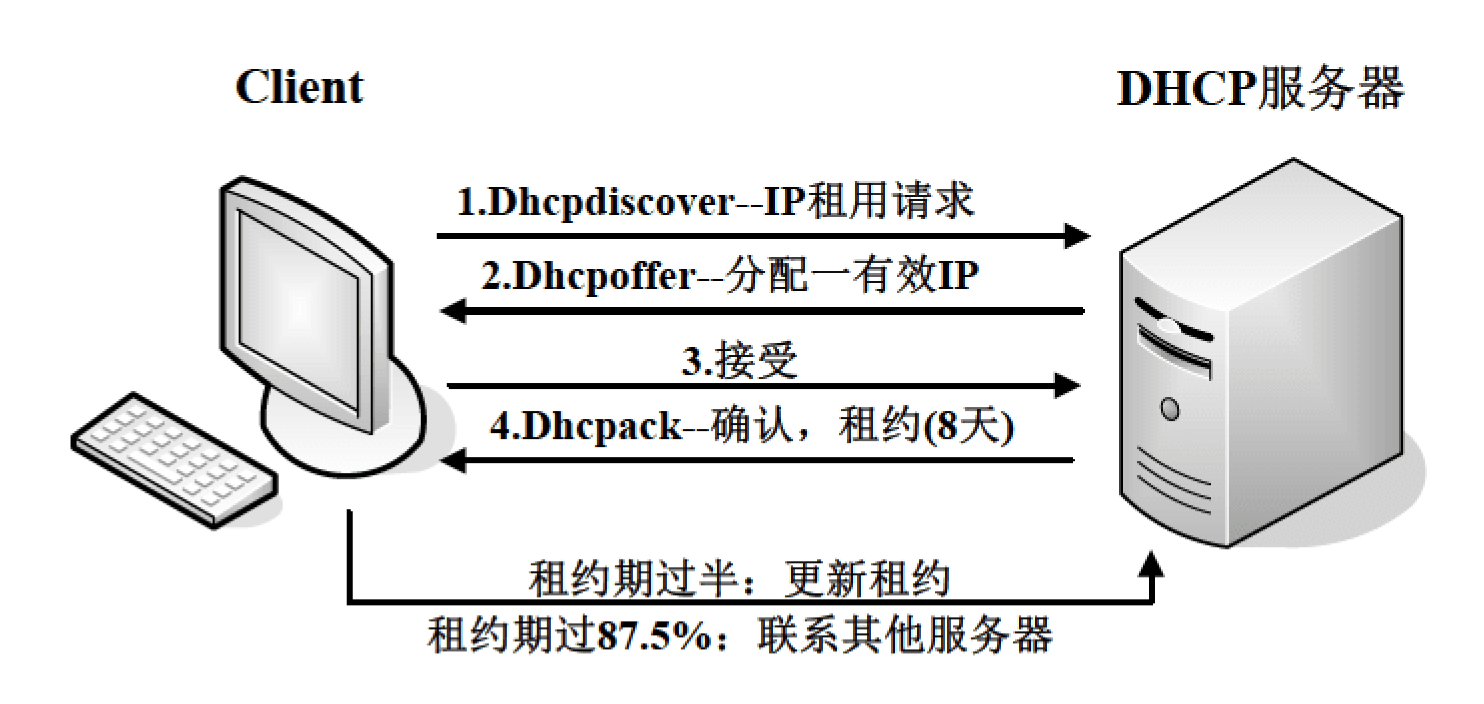


图 4-2　DHCP 服务过程

不论是 DHCP 客户还是 DHCP 服务器，都是通过按 DHCP 消息格式要求来填写各个段形成具体的 DHCP 消息，DHCP 用的传输协议的非面向连接的 UDP（用户数据报协议），从 DHCP 客户发出的 DHCP 消息送往 DHCP 服务器的端口 67，DHCP 服务器发给客户的 DHCP 消息送往 DHCP 客户的端口 68，由于在取得服务器赋予的 IP 之前，DHCP 客户并没有自己的 IP，所以包含 DHCP 消息的 UDP 数据报的 IP 头的源地址段是 0.0.0.0，目的地址则是 255.255.255.255。

4.3.6　代理服务器的基本原理

代理服务器是介于浏览器和服务器之间的另一台服务器，是网络信息的中转站。使用代理功能后，浏览器将首先向代理服务器发送请求，进而由代理服务器完成请求内容，将数据再返回给浏览器。

一般说来，代理服务器具有以下的功能：

（1）通过缓存增加访问速度。

通过代理服务器的缓存功能来加快网络的访问速度。一般说来，大多数的代理服务器都支持 HTTP 缓存，但是，有的代理服务器也支持 FTP 缓存。在选择代理服务器时，对于大多数的组织，只需要 HTTP 缓存功能就足够了。

（2）提供用私有 IP 访问 Internet 的方法。

IP 地址是不可再生的宝贵资源，假如你只有有限的 IP 地址，但是需要提供整个组织的 Internet 访问能力，那么，你可以通过使用代理服务器来实现这一点。

（3）提高网络的安全性。

如果内部用户访问 Internet 都是通过代理服务器，那么，代理服务器就成为进入 Internet 的唯一通道；反过来说，代理服务器也是 Internet 访问内部网的唯一通道，如果没有反向代理，则对于 Internet 上的主机来说，整个内部网只有代理服务器是可见的，从而大大增强了网络的安全性。

4.4 例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 7 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

用于支持在电子邮件中传送音频和图像的协议是__（1）__。

（1）A. SMTP　　B. POP　　C. MIME　　D. POP3

例题 1 分析

题中选项 SMTP（简单邮件传输协议）、POP（邮局协议）、POP3（邮局协议 V3）均是收发邮件的标准协议，而 MIME（多用途互联网邮件扩展）是最初的互联网电子邮件协议的一个扩展，使人们能使用这一协议在互联网上交换不同类型的数据文件：音频、视频、图像、应用软件和其他类型的文件，也包括在最初的协议——简单邮件传送协议（SMTP）中的 ASCII 文本。对 SMTP 进行扩展以使互联网（主要是网站）用户和服务商能识别和处理除 ASCII 文本以外其他类型的数据。结果，新的文件类型作为一个互联网协议文件的支持类型补充到“邮件”中。服务商在任意的网站传播物中插入 MIME 标题。用户使用这一标题来选择适合播放标题所表示的文件类型的应用软件。一些这样的播放器被装于网络客户机或浏览器中（比如，所有的浏览器都包含有 GIF 和 JPEG 图像浏览器，并有处理 HTML 文件的能力）；其他的播放器可能需要下载。

例题 1 答案

（1）C

例题 2

__（2）__命令可实现重新启动 Linux 操作系统。

（2）A. init 0　　B. halt　　C. shutdown –r　　D. shutdown –h

例题 2 分析

Linux 中常用的关机和重新启动命令有 shutdown、halt、reboot 以及 init，它们都可以达到关机和重新启动的目的，但是每个命令的内部工作过程是不同的，下面将逐一进行介绍。

1）shutdown

shutdown 命令用于安全关闭 Linux 系统。执行 shutdown 命令时，系统会通知所有登录的用户系统将要关闭，并且 login 指令会被冻结，即新的用户不能再登录系统。使用 shutdown 命令可以直接关闭系统，也可以延迟指定的时间再关闭系统，还可以重新启动。延迟指定的时间再关闭系统，可以让用户有时间储存当前正在处理的文件和关闭已经打开的程序。

shutdown 命令的部分参数如下：

[-t] 指定在多长时间之后关闭系统；

[-r] 重启系统；

[-k] 并不真正关机，只是给每个登录用户发送警告信号；

[-h] 关闭系统（halt）。

shutdown 命令的工作实质是给 init 程序发送信号（signal），要求其切换系统的运行级别（Runlevel）。系统的运行级别包括：

0：关闭系统；

1：单用户模式，如果没有为 shutdown 命令指定-h 或-r 参数而直接执行，则默认将切换到此运行级别；

2：多用户模式（不支持 NFS）；

3：多用户模式（支持 NFS），一般常用此种运行级别；

5：多用户模式（GUI 模式）；

6：重新启动系统。

2）halt

halt 是最简单的关机命令，其实际上是调用 shutdown -h 命令。halt 执行时，杀死应用进程，文件系统写操作完成后就会停止内核。halt 命令的部分参数如下：

[-f] 没有调用 shutdown 而强制关机或重启；

[-i] 关机或重新启动之前，关掉所有的网络接口；

[-p] 关机时调用 poweroff，此选项为默认选项。

3）reboot

reboot 的工作过程与 halt 类似，其作用是重新启动，而 halt 是关机。其参数也与 halt

类似。

4）init

init 是所有进程的祖先，其进程号始终为 1。init 用于切换系统的运行级别，切换的工作是立即完成的。init 0 命令用于立即将系统运行级别切换为 0，即关机；init 6 命令用于将系统运行级别切换为 6，即重新启动。

例题 2 答案

（2）C

例题 3

下面顶级域名中表示政府机构的是__（3）__。

（3）A. mil　　B. edu　　C. gov　　D. org

例题 3 分析

本题考查因特网应用中顶级域名的相关定义。顶级域名又分为组织域名与国家或地区域名。常见组织域名及代表的意义如下：

- .com：Commercial organizations，商业组织，公司；
- .edu：Educational institutions，教研机构；
- .gov：Governmental entities，政府部门；
- .int：International organizations，国际组织；
- .mil：Military（U.S），美国军部；
- .net：Network operations and service centers，网络服务商；
- .org：Other organizations，非盈利组织。

例题 3 答案

（3）C

例题 4

FTP 使用的传输层协议为__（4）__；FTP 有 2 个端口，其中用作控制连接的号为默认端口为__（5）__，用作数据传输的默认端口号为__（6）__。

（4）A. HTTP　　B. IP　　C. TCP　　D. UDP

（5）A. 80　　B. 25　　C. 445　　D. 21

（6）A. 80　　B. 25　　C. 20　　D. 445

例题 4 分析

FTP 文件传送协议，是一个用于从一台主机传送文件到另一台主机的协议。与大多数 Internet 服务一样，FTP 也是一个客户机/服务器系统。它是面向可靠的，面向连接的文件传输协议，它是基于网络层 TCP 协议来传输文件的。这也是它与 TFTP 协议的不同之处，TFTP 是提供无连接的，不可靠的数据传输（基于 UDP 协议）。FTP 通过两个端口进行通信，一个为控制端口（21），一个为数据传输端口（20）。

例题 4 答案

（4）C　（5）D　（6）C

例题 5

某 Internet 主页的 URL 地址为 http://www.csai.cn/product/index.html，该地址的域名是__（7）__。

（7）A．index.html　　B．com.cn

C．www.csai.cn　　D．http://www.csai. cn

例题 5 分析

本题是一个考察 URL 基本格式的概念题，在 URL 中，通常是以协议打头，接下来是主机域名或 IP 地址，再接下来是服务器上的资源文件夹路径，最后是具体要访问的资源。此处很明显地知道域名是 www.csai. cn。

例题 5 答案

（7）C

例题 6

在 WWW 服务器与客户机之间发送和接收 HTML 文档时，使用的协议是__（8）__。

（8）A．FTP　　B．Gopher　　C．HTTP　　D．NNTP

例题 6 分析

HTTP：超级文本传输协议的缩写，用于管理超级文本与其他超级文本文档之间的连接。

Gopher 是基于菜单驱动的 Internet 信息查询工具，它可以将用户的请求自动转换成 FTP 或 Telnet 命令。在一级一级菜单的导引下，用户通过选取自己感兴趣的信息资源，就可以对 Internet 网上的远程机信息系统进行实时访问，这对于不熟悉网络资源、网络地址和网络查询命令的用户是十分方便的。

NNTP：网络新闻传输协议是一个广泛使用的协议。它提供通常作为 USENET 新闻组的新闻服务。NNTP 定义了使用一个可靠的建立在流基础上的，在 Internet 上传输新闻的分发、询问、获取和发布的一个协议。NNTP 被设计成新闻，被存储在一个中心数据库，允许订阅者选择他们希望读的主题。目录，交叉引用和过期的新闻都能找到。NNTP 有许多特性和简单邮件传输协议及 TCP 相似。与 SMTP 的相似之处在于它能接受一般的英语命令。与 TCP 的相似之处在于它是建立在流的传输和分发的基础上的。NNTP 通常在端口 119 运行。

例题 6 答案

（8）C

例题 7

Internet 中域名与 IP 地址之间的翻译是由__（9）__来完成的。

（9）A．DNS 服务器　　B．代理服务器　　C．FTP 服务器　　D．Web 服务器

例题 7 分析

DNS 也称为域名服务，即实现 IP 地址与更易记的域名进行翻译转换的应用；代理服务器是“代理”局域网内计算机访问 Internet 的服务器；FTP 是用来完成文件传输的；Web 服务器是负责提供万维网服务的。

例题 7 答案

（9）A

第 5 章　网络管理基础

根据网络管理员的考试大纲要求，本章应掌握网络管理基本概念、协议与工具，掌握网络操作系统的配置与维护等相关的基础知识。

从历年试题来看，本章的出题数在 9 分左右，占上午考试的 12%左右。本章的考题分布主要来自于 OSI 网络管理标准、SNMP 协议规范、Windows/Linux 网络基础配置与管理、网络故障诊断命令的使用等知识点。

5.1　网络管理基本概念

在网络的早期阶段，当计算机网络还处于研究阶段而不是供数以百万计的人们使用的网络体系时期，“网络管理”还是一个非常超前的概念。随着大规模网络的快速增长，网络复杂性和异构性的特点日益突出，使得网络管理（通常简称为“网管”）问题上升到网络建设的战略性地位，研究符合当前需要的、经济适用的网络管理途径是一项迫切的任务。

5.1.1　网络管理的基本定义

虽然网络管理还没有精确的定义，但它的内容可归纳为：

网络管理包括对硬件、软件和人力的使用、综合与协调，以便对网络资源进行监视、测试、配置、分析、评价和控制，这样就能以合理的价格满足网络的一些需求，如实时运行性能、服务质量等。网络管理常简称为网管。

5.1.2　网络管理的分类

事实上，网络管理技术是伴随着计算机、网络和通信技术的发展而发展的，两者相辅相成。从网络管理范畴来分类，可分为对网“路”的管理，即针对交换机、路由器等主干网络进行管理；对接入设备的管理，即对内部 PC、服务器、交换机等进行管理；对行为的管理，即针对用户的使用进行管理；对资产的管理，即统计 IT 软硬件的信息等。根据网管软件的发展历史，可以将网管软件划分为三代：

第一代网管软件就是最常用的命令行方式，并结合一些简单的网络监测工具，它不仅要求使用者精通网络的原理及概念，还要求使用者了解不同厂商的不同网络设备的配置方法。

第二代网管软件有着良好的图形化界面。用户无需过多了解设备的配置方法，就能

图形化地对多台设备同时进行配置和监控，大大提高了工作效率，但仍然存在由于人为因素造成的设备功能使用不全面或不正确的问题，容易引发误操作。

第三代网管软件相对来说比较智能，是真正将网络和管理进行有机结合的软件系统，具有“自动配置”和“自动调整”功能。对网管人员来说，只要把用户情况、设备情况及用户与网络资源之间的分配关系输入网管系统，系统就能自动地建立图形化的人员与网络的配置关系，并自动鉴别用户身份，分配用户所需的资源（如电子邮件、Web、文档服务等）。

5.1.3 网络管理的标准和协议

随着对网络管理系统的迫切需求和网络管理技术的日渐成熟，为了适应网络异构互联、资源共享的发展趋势。ISO 开始制定关于网络管理的国际标准。

本小节主要从标准 CMIS/CMIP 协议的角度来宏观理解网络管理，并重点掌握 SNMP 网络管理协议，了解诸如 CMOT、RMON、TMN 等其他常用的网络管理协议。

1．CMIS/CMIP 协议

公共管理信息服务（CMIS）/公共管理信息协议（CMIP）是 OSI 所提供的网络管理协议族，它定义了每个网络组成部分提供的网络管理服务。它和 SNMP 的最大不同是，SNMP 的原则是简单、易于实现，而 CMIS/CMIP 在于完整的网络管理方案。

CMIS/CMIP 中的网络管理应用进程使用的是 ISO 参考模型中的应用层。在该层上，由公共管理信息服务单元（CMISE）提供应用程序使用 CMIP 的接口，并提供了联系控制服务元素（ACSE，在应用程序间建立和关闭联系）和远程操作服务元素（ROSE，处理应用间的请求/响应交互）两个协议。

2．SNMP 协议

本知识点重点在于了解 SNMP 协议组的构建，管理模型的构成、各版本的区别、MIB 基础知识，要求掌握 SNMP 的协议基础、特点以及 5 种常见协议数据单元的功能与特点。

1）SNMP 协议和版本区别

SNMP 是基于 TCP/IP 协议族的网络管理标准，它的前身是 SGMP（简单网关监控协议），SNMPv1 是 IETF 在 1990 年发布的，后来又发布了 SNMPv2、SNMPv3。具体描述请参考表 5-1。

表 5-1 SNMP 三个版本

版　本	描　述
V1	由于轮询的性能限制，SNMP 不适合管理很大的网络。SNMP 不适合检索大量数据。SNMP 的陷入报文是没有应答的，可能会丢掉重要的管理信息。SNMP 只提供简单的团体名认证，安全措施很弱。不支持管理站之间的通信

续表

版　本	描　述
V2	管理者与管理者之间可以通信。SNMPv2 提供三种访问管理信息的方法：管理站和代理之间的请求/响应通信；代理系统到管理站的非确认通信；管理站和管理站之间的请求/响应通信，以支持分布式网络管理
V3	提供了数据源标识、报文完整性认证、防止重放、报文机密性、授权和访问控制、远程配置与高层管理

2）MIB 与 MIB-2

SNMP 是一组协议标准，它主要包括管理信息库（MIB）、管理信息结构（SMI）和管理通信协议（SNMP）三个部分。其网络管理模型则是由管理进程（Manager，处于管理模型核心，负责完成网管各项功能）、代理（Agent，运行在设备上的管理程序，负责收集信息）、管理信息库三个部分组成的。

MIB 是网络管理系统中的重要构件，由系统内许多被管理的对象及属性组成，它是一个虚拟的数据库，采用树型结构组织。它经历了 MIB-1 和 MIB-2 两个版本。MIB-2 定义了系统组（System）、接口组（Interface）、地址转换组（AddressTranslation）、IP 组、ICMP 组、TCP 组、UDP 组、EGP 组、传输组（Transmission）和 SNMP 等 11 个功能组。SNMP 现在使用的是 MIB-2。

3）SNMP 协议的工作模式

SNMP 使用 UDP 作为传输协议，是一种异步的请求/响应协议，其默认端口有两个：一是用于数据传送与接收的 161 号端口；二是用于报警（Trap）信息接收的 162 号端口。

SNMPv1 使用了五种格式的 PDU（协议数据单元），也是 SNMP 系列协议中最基础部分：

- Get-Request：由管理进程发送，向管理代理请求它们的取值。
- Get-NextRequest：由管理进程发送，是在 Get-Request 报文后使用，表示查询 MIB 中的下一个对象，常用于循环查询。
- Set-Request：由管理进程发出，用来请求改变管理代理上的某些对象。
- Get-Response：当管理代理收到管理进程发送的 Get-Request 或 Get-NextRequest 报文时，将应答一个该报文。

注：以上 4 种均为简单的请求/响应机制，前三个都是原子操作。

- Trap：是这一种报警机制（即属于无请求的），用于意外或突发故障情况下，管理代理主动向管理进程发送报警信息。常见的报警类型有：冷启动、热启动、线路故障、线路故障恢复、认证失败等。

与 SNMPv1 不同的是，SNMPv2 不仅支持管理站（管理进程）与管理代理进行请求/响应通信，还允许管理站之间进行通信。

3．RMON 及其他协议

RMON（远程网络监控协议）也是一种监控局域网通信的标准。它在 SNMP 管理信

息库的基础上进行了扩充。它能够实现离线操作、主动监视、问题检测和报告、提供增值数据、多管理站操作等。RMON 的目标是为了扩展 SNMP 的 MIB-II（管理信息库），使 SNMP 更为有效、更为积极主动地监控远程设备。RMON MIB 由一组统计数据、分析数据和诊断数据构成，利用许多供应商生产的标准工具都可以显示出这些数据，因而它具有独立于供应商的远程网络分析功能。

RMON 规范的大部分是 RMON 管理信息库（RMON MIB）的定义，这一 MIB 现已被吸收进 MIB-II，其子树标识符是 16。RMON MIB 的结构分为 9 组：

（1）统计（Statistics）：维护代理监视的每一子网的基本使用和错误统计。

（2）历史（History）：记录从统计组可得到的信息的周期性统计样本。

（3）警报（Alarm）：允许管理控制台人员为 RMON 代理记录的任何记数和整数设置采样间隔和报警阀值。

（4）主机（Host）：包括关于连接到子网上的主机的各种流量的计数。

（5）最高 N 台主机（HostTopN）：包含排序后的主机统计。

（6）矩阵（Matrix）：以矩阵形式显示出错和使用信息。

（7）过滤（Filter）：允许监视器观测与一过滤器相匹配的数据包。

（8）包捕获（Packet capture）：控制数据被发往管理控制台的方式。

（9）事件（Event）：一个关于由 RMON 代理产生的所有事件的表。

RMON MIB 中的所有组都是可选的，但它们之间有一些依赖性：警报组需要事件组的实现。最高 N 台组（hostTopN）需要主机组的实现。包捕获组需要过滤组的实现。

除了理论标准 CMIS/CMIP 和事实标准 SNMP 外，常见的其他网管协议规范还包括：

（1）CMOT：公共管理信息服务与协议，它在 TCP/IP 协议族上实现了 CMIS 服务。它是一个过渡性解决方案，提供给想过渡到 OSI 网络管理协议的用户使用。

（2）LMMP：局域网个人管理协议，试图为 LAN 环境提供一个网络管理方案，它工作在 LLC 层，不依赖于任何特定的网络协议，它更容易实现，但不能够跨越路由器。

（3）TMN：电信管理网（M.30 建议），目的是利用既简单又统一的方法来管理各种不同功能的网络。TMN 的最大优势在于其信息模型的标准化：统一多厂家设备的规范管理；而其最大的不足是处理时延长，不能够满足一些实时处理的要求，而且它是工作在网元级的，没有站在全网的基础上建模。近年来，最新的发展是使用 CORBA 技术来完善 TMN。

（4）基于 CORBA 的网络管理：2000 年版的 M.3010 和 M.3013 为 CORBA 技术引入到以 TMN 为基础的网络管理框架中铺平了道路；X.780 和 Q.816 分别规定了采用细粒度方法的基于 CORBA 技术的网络管理接口定义指南和所需 CORBA 服务；X.780.1 和 Q.816.1 分别规定了采用粗粒度方法的基于 CORBA 技术的网络管理接口定义指南和所需 CORBA 服务。

5.2　网络管理基本命令

本节介绍的知识点主要有 Windows/Linux 操作系统下网络故障的诊断及相应的诊断命令的使用。

1．Windows 网络诊断命令

（1）ipconfig 命令：用于显示 TCP/IP 配置，以下是一些常见的命令选项。

```
ipconfig/all 显示所有配置信息
ipconfig/release 释放 IP 地址
ipconfig/renew 重新获得一个 IP 地址，会向 DHCP 服务器发出新请求
ipconifg/flushdns 清空 DNS 解析器缓存
ipconfig/registerdns 更新所有 DHCP 租约并重新注册 DNS 域名
ipconfig/displaydns 显示 DNS 解析器缓存
ipconfig/setclassid 设置 DHCP 类 ID
```

（2）ping 命令：基于 ICMP 协议，用于把一个测试数据包发送到规定的地址，如果一切正常则返回成功响应。它常用于以下几个情形：

- 验证 TCP/IP 协议是否正常安装：ping 127.0.0.1，如果正常返回，说明安装成功。其中 127.0.0.1 是回送地址。
- 验证 IP 地址配置是否正常：ping 本机 IP 地址。
- 查验远程主机：ping 远端主机 IP 地址。

（3）nbtstat：用于显示 NetBIOS 协议的统计，及 NetBIOS 地址与 IP 地址的对应关系。

（4）netstat：网络状态查看命令，以下是一些常见的命令选项。

```
netstat-a 显示所有连接和监听端口
netstat-e 显示以太网统计
netstat-n 以数字格式显示 IP 地址
netstat-o 显示每个连接所属的处理 ID
netstat-p 显示特定协议的连接
netstat-r 显示路由表
netstat-s 显示每个协议统计
```

（5）tracert：用于查看分组传链路路径。Tracert 将包含不同生存时间（TTL）值的 Internet 控制消息协议（ICMP）回显数据包发送到目标，以决定到达目标采用的路由。要在转发数据包上的 TTL 之前至少递减 1，必需路径上的每个路由器，所以 TTL 是有效的跃点计数。数据包上的 TTL 到达 0 时，路由器应该将“ICMP 已超时”的消息发送回源系统。Tracert 先发送 TTL 为 1 的回显数据包，并在随后的每次发送过程中将 TTL 递

增 1，直到目标响应或 TTL 达到最大值，从而确定路由。路由通过检查中级路由器发送回的“ICMP 已超时”的消息来确定路由。不过，有些路由器悄悄地下传包含过期 TTL 值的数据包，而 tracert 看不到。

```
tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name
```

参数说明：

/d 指定不将地址解析为计算机名。

-h maximum_hops 指定搜索目标的最大跃点数。

-j computer-list 指定沿 computer-list 的稀疏源路由。

-w timeout 每次应答等待，timeout 指定的微秒数。

target_name 目标计算机的名称。

2．Linux 网络诊断命令

（1）ifconfig 命令：用于查看和更改网络接口的地址和参数，包括 IP 地址、网络掩码、广播地址，使用权限是超级用户。格式如下：

```
ifconfig -interface[options] address
```

主要参数：

-interface：指定的网络接口名，如 eth0 和 eth1。

up：激活指定的网络接口卡。

down：关闭指定的网络接口。

Broadcast address：设置接口的广播地址。

pointopoint：启用点对点方式。

address：设置指定接口设备的 IP 地址。

netmask address：设置接口的子网掩码。

（2）ip 命令：是 iproute 2 软件包里面的一个强大的网络配置工具，它能够替代一些传统的网络管理工具，例如 ifconfig、route 等，使用权限为超级用户。格式如下：

```
ip [OPTIONS] OBJECT [COMMAND [ARGUMENTS]]
```

主要参数：

OPTIONS 是修改 ip 行为或改变其输出的选项。所有的选项都是以-字符开头，分为长、短两种形式。

OBJECT 是要管理者获取信息的对象。

COMMAND 设置针对指定对象执行的操作，它和对象的类型有关。

ARGUMENTS 是命令的一些参数，它们依赖于对象和命令。

（3）ping 命令：检测主机网络接口状态，使用权限是所有用户。这个 Ping 的过程实

际上就是 ICMP 协议工作的过程。还有其他的网络命令如跟踪路由的 Tracert 命令也是基于 ICMP 协议的。格式如下：

```
ping [-dfnqrRv][-c][-i][-I][-l][-p][-s][-t] IP 地址
```

主要参数：

-d：使用 Socket 的 SO_DEBUG 功能。
-c：设置完成要求回应的次数。
-f：极限检测。
-i：指定收发信息的间隔秒数。
-I：网络界面使用指定的网络界面送出数据包。
-l：前置载入，设置在送出要求信息之前，先行发出的数据包。
-n：只输出数值。
-p：设置填满数据包的范本样式。
-q：不显示指令执行过程，开头和结尾的相关信息除外。
-r：忽略普通的 RoutingTable，直接将数据包送到远端主机上。
-R：记录路由过程。
-s：设置数据包的大小。
-t：设置存活数值 TTL 的大小。
-v：详细显示指令的执行过程。

（4）netstat 命令：作用检查整个 Linux 网络状态，格式如下：

```
netstat [-acCeFghilMnNoprstuvVwx][-A][--ip]
```

主要参数：

-a--all：显示所有连线中的 Socket。
-A：列出该网络类型连线中的 IP 相关地址和网络类型。
-c--continuous：持续列出网络状态。
-C--cache：显示路由器配置的快取信息。
-e--extend：显示网络其他相关信息。
-F--fib：显示 FIB。
-g--groups：显示多重广播功能群组组员名单。
-h--help：在线帮助。
-i--interfaces：显示网络界面信息表单。
-l--listening：显示监控中的服务器的 Socket。
-M--masquerade：显示伪装的网络连线。
-n--numeric：直接使用 IP 地址，而不通过域名服务器。

-N--netlink--symbolic：显示网络硬件外围设备的符号连接名称。

-o--timers：显示计时器。

-p--programs：显示正在使用 Socket 的程序识别码和程序名称。

-r--route：显示 RoutingTable。

-s--statistice：显示网络工作信息统计表。

-t--tcp：显示 TCP 传输协议的连线状况。

-u--udp：显示 UDP 传输协议的连线状况。

-v--verbose：显示指令执行过程。

-V--version：显示版本信息。

-w--raw：显示 RAW 传输协议的连线状况。

-x--unix：和指定“-Aunix”参数相同。

--ip--inet：和指定“-Ainet”参数相同。

（5）telnet 命令：telnet 表示开启终端机阶段作业，并登入远端主机。telnet 是一个 Linux 命令，同时也是一个协议（远程登录协议）。格式如下：

```
telnet [-8acdEfFKLrx][-b][-e][-k][-l][-n][-S][-X][主机名称 IP 地址<通信端
口>]
```

主要参数：

-8：允许使用 8 位字符资料，包括输入与输出。

-a：尝试自动登入远端系统。

-b：使用别名指定远端主机名称。

-c：不读取用户专属目录里的.telnetrc 文件。

-d：启动排错模式。

-e：设置脱离字符。

-E：滤除脱离字符。

-f：此参数的效果和指定“-F”参数相同。

-F：使用 KerberosV5 认证时，加上此参数可把本地主机的认证数据上传到远端主机。

-k：使用 Kerberos 认证时，加上此参数让远端主机采用指定的领域名，而非该主机的域名。

-K：不自动登入远端主机。

-l：指定要登入远端主机的用户名称。

-L：允许输出 8 位字符资料。

-n：指定文件记录相关信息。

-r：使用类似 rlogin 指令的用户界面。

-S：服务类型，设置 telnet 连线所需的 IPTOS 信息。

-x：假设主机有支持数据加密的功能，就使用它。

-X：关闭指定的认证形态。

（6）route 命令：表示手工产生、修改和查看路由表。格式如下：

```
#route  [-add][-net|-host]targetaddress[-netmaskNm][dev]If]
#route  [—delete][-net|-host]targetaddress[gwGw][-netmaskNm][dev]If]
```

主要参数：

-add：增加路由。

-delete：删除路由。

-net：路由到达的是一个网络，而不是一台主机。

-host：路由到达的是一台主机。

-netmaskNm：指定路由的子网掩码。

gw：指定路由的网关。

[dev]If：强迫路由链指定接口。

（7）nslookup 命令：查询一台机器的 IP 地址和其对应的域名。使用权限所有用户。它通常需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器，就可以用这个命令查看不同主机的 IP 地址对应的域名。格式如下：

```
nslookup [IP 地址/域名]
```

5.3　网络故障分析与维护

本知识点重点在于了解各种网络故障的类型，掌握标准的排错思路，建立排错的宏观概念。网络中可能出现的故障多种多样，往往解决一个复杂的网络故障需要广泛的网络知识与丰富的工作经验。由于网络故障的多样性和复杂性，网络故障分类方法也不尽相同，了解不同类型的故障对于解决与排除是十分重要的。

1．网络故障的划分

根据网络故障不同性质可划分物理故障和逻辑故障，详情见表 5-2。

表 5-2　不同性质的网络故障

类　　别	典 型 代 表	解决思路/案例
物理故障	设备或线路损坏、插头松动、线路受到严重电磁干扰	通过 ping 来检查端口的连通性，查出相应的插头及线路进行修正
	网络插头误接	十分隐蔽，没有特别好的工具
逻辑故障	配置错误	例如路由器端口参数设定有误，使用 tracerouter 工具寻找诸如路由循环的问题
	重要进程端口关闭，以及系统的负载过高	检查其端口状态

根据网络故障不同对象划分为线路故障、路由器故障和主机错误，详情见表 5-3。

表 5-3 不同对象的网络故障

类　　别	典 型 代 表	解决思路/案例
线路故障	线路不通	通过 Ping 命令检查端口
	路由器配置错误	使用 tracerouter 检查
路由器故障	路由器硬件错误（CPU 温度过高，内存余量太小）	使用 MIB 变量浏览器检查
	配置错误	情况复杂，在后面知识点介绍
主机错误	主机配置不当（如 IP 地址）	逐一检查
	安全故障（启动了多余服务）	通过端口扫描、入侵检测等

2．故障排除的标准过程

虽然网络的故障种类繁多，涉及面广、复杂，但对于大多数故障而言，故障排除的主要过程还是十分接近的：

- 找出与故障有关的信息。
- 忽略与故障无关的信息。
- 推断、精确测定和隔离问题区域。
- 设计一个纠正的行动解决方案以修复问题。

在实际的解决过程中，我们可以采用分层诊断技术，具体地说，就是从物理层开始，逐层地分析、排除。详情见表 5-4。

表 5-4 排错过程

层　　次	常见故障现象	关 键 手 段
物理层	设备的物理连接方式是否恰当，连接电缆是否正确	使用 showinterface（路由器）、ipconfig/all（Windows 主机）、ifconfig（Linux 主机）来检查
数据链路层	体现在数据封装协议、通道设置等方面的问题	查看路由器接口的协议配置
网络层	路由选择错误、连接错误等	沿着从源到目标的路径，检查路由表、接口 IP 地址

3．单机网络故障的排除

单机网络故障产生的原因主要包括软件和硬件两个方面，我们可以采用如下所示的方法进行逐一地排查。

1）硬件方面

硬件故障主要有网卡自身故障、网卡未正确安装、网卡故障、集线器故障等。通常首先检查插上计算机 I/O 插槽上的网卡侧面的指示灯是否正常，网卡一般有两个指示灯“连接指示灯”和“信号传输指示灯”，正常情况下“连接指示灯”应一直亮着，而“信号传输指示灯”在信号传输时应不停闪烁。如“连接指示灯”不亮，应考虑连接故障，即网卡自身是否正常，安装是否正确，网线、集线器是否有故障。对于网卡的部分，我

们应先检测以下两个最常见的问题：

（1）RJ45 接头的问题。

RJ45 接头容易出故障，例如，双绞线的头没顶到 RJ-45 接头顶端，绞线未按照标准脚位压入接头，甚至接头规格不符或者是内部的绞线断了。

镀金层厚度对接头品质的影响也是相当可观的，例如镀得太薄，那么网线经过三五次插拔之后，也许就把它磨掉了，接着被氧化，当然也容易发生断线。

（2）接线故障或接触不良。

一般可观察下列几个地方：双绞线颜色和 RJ-45 接头的脚位是否相符；线头是否顶到 RJ-45 接头顶端，若没有，该线的接触会较差，需再重新压按一次；观察 RJ-45 侧面。金属片是否已刺入绞线之中？若没有，极可能造成线路不通；观察双绞线外皮去掉的地方，是否使用剥线工具时切断了绞线（绞线内铜导线已断，但皮未断）。

如果还不能发现问题，那么我们可用替换法排除网线和集线器故障，即用通信正常的计算机的网线来连接故障机，如能正常通信，显然是网线或集线器的故障，再转换集线器端口来区分到底是网线还是集线器的故障，许多时候集线器的指示灯也能提示是否是集线器故障，正常对应端口的灯应亮着。

2）软件方面

如果网卡的信号传输指示灯不亮，这一般是由网络的软件故障引起的。

（1）检查网卡设置。

普通网卡的驱动程序磁盘大多附有测试和设置网卡参数的程序。分别查验网卡设置的接头类型、IRQ、I/O 端口地址等参数，若有冲突，只要重新设置（有些必须调整跳线），一般都能使网络恢复正常。

另外检查一下网卡驱动程序是否正常安装。不同网卡使用的驱动程序亦不尽相同，假如你选错了，就有可能发生不兼容的现象。修复的方法亦不难，只要找到正确的驱动程序，重新安装即可。

最后我们简单检验一下网卡设置故障是否排除。打开“控制面板-系统-设备管理器”，选中我们安装的网络适配器，单击“属性”按钮，在“常规”选项卡中，可以查看网卡是否在正常工作。

（2）检查网络协议。

打开“控制面板-网络-配置”选项，查看已安装的网络协议，必须配置以下各项：NetBEUI 协议和 TCP/IP 协议，Microsoft 友好登录，拨号网络适配器。如果以上各项都存在，重点检查 TCP/IP 是否设置正确。在 TCP/IP 属性中要确保每一台计算机都有唯一的 IP 地址，将子网掩码统一设置为 255.255.255.0，网关要设为代理服务器的 IP 地址（如 192.168.0.1）。另外必须注意主机名在局域网内也应该是唯一的。最后，我们用 ping 命令来检验一下网卡能否正常工作。

```
ping 127. 0. 0. 1
```

127.0.0.1 是本地循环地址。如果该地址无法 ping 通，则表明本机 TCP/IP 协议不能正常工作；如果 ping 通了该地址，证明 TCP/IP 协议正常，则进入下一个步骤继续诊断。

（3）ping 本机的 IP 地址。

使用 ipconfig 命令可以查看本机的 IP 地址，ping 该 IP 地址，如果 ping 通，表明网络适配器（网卡或者 Modem）工作正常，则需要进入下一个步骤继续检查；反之则是网络适配器出现故障。

（4）ping 本地网关。

本地网关的 IP 地址是已知的 IP 地址。ping 本地网关的 IP 地址，ping 不通则表明网络线路出现故障。如果网络中还包含有路由器，还可以 ping 路由器在本网段端口的 IP 地址，不通则此段线路有问题，通则再 ping 路由器在目标计算机所在同段的端口 IP 地址，不通则是路由出现故障。如果通，最后再 ping 目的机的 IP 地址。

（5）ping 网址。

如果要检测的是一个带 DNS 服务的网络（比如 Internet），上一步 ping 通了目标计算机的 IP 地址后。仍然无法连接到该机，则可以 ping 该机的网络名，比如：pingwww.csai.cn，正常情况下会出现该网址所指向的 IP 地址，这表明本机的 DNS 设置正确而且 DNS 服务器工作正常，反之就可能是其中之一出现了故障。

5.4 例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 7 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

ISO 定义的网络管理功能中，__（1）__的功能包括初始化被管理对象、更改系统配置等。

（1）A. 配置管理　　B. 故障管理　　C. 性能管理　　D. 安全管理

例题 1 分析

ISO 定义了配置管理、故障管理、性能管理、安全管理和计费管理五个功能域。

配置管理（configuration management）：初始化网络、配置网络，以使其提供网络服务。配置管理，是一组对辨别、定义、控制和监视组成一个通信网络的对象所必要的相关功能，目的是为了实现某个特定功能或使网络性能达到最优。

故障管理（fault management）：检测、记录、通知用户，且有可能的话，自动修复网络问题，保持网络有效地运行。网络故障管理包括故障检测、隔离和纠正三方面。

性能管理（performance management）：测量和跟踪网络变量，实现网络性能监控和优化。其能力包括监视和分析被管网络及其所提供服务的性能机制。性能分析的结果可能会触发某个诊断测试过程或重新配置网络以维持网络的性能。性能管理收集分析有关

被管网络当前状况的数据信息，并维持和分析性能日志。

安全管理（security management）：控制网络资源的访问权限，从而不会导致网络遭到破坏。只有被授权的用户才有权访问敏感信息。

计费管理（accounting management）：测量网络利用情况，这样可以追踪和调整网络资源的个人或组使用。主要负责网络使用规则和账单等。

例题 1 答案

（1）A

例题 2

在 TCP/IP 网络管理中，MIB 数据库中的信息是由__（2）__来收集的。

（2）A. 管理站（Manager）　　B. 代理（Agent）

C. Web 服务器（Web Server）　　D. 浏览器（Browser）

例题 2 分析

管理信息库（Management Information Base，MIB）可以从支持 SNMP 的代理端收集信息，并通过图形显示例如接口流量和 CPU 负载等性能参数，从而实现实时监控。

网络管理的实现过程如下，管理工作站主动向代理发送请求，要求得到关心的数据。代理在接到管理工作站的请求之后，响应管理工作站的请求，把数据发送给管理工作站。这种收集数据的方式称为轮询。除此之外，被管理设备中的代理可以在任何时候向网络管理工作站报告错误情况，这是基于中断的方式，又称为自陷。

例题 2 答案

（2）B

例题 3

在 Windows 操作系统中运行__（3）__命令可观察本机当前所有连接及端口等信息。

（3）A. arp　　B. tracert　　C. nslookup　　D. netstat

例题 3 分析

netstat 命令的功能是显示网络连接、路由表和网络接口信息，可以让用户得知目前都有哪些网络连接正在运作。该命令的一般格式为：netstat [选项]

命令中各选项的含义如下：

-a 显示所有 socket，包括正在监听的。

-c 每隔 1 秒就重新显示一遍，直到用户中断它。

-i 显示所有网络接口的信息，格式同“ifconfig -e”。

-n 以网络 IP 地址代替名称，显示出网络连接情形。

-r 显示核心路由表，格式同“route -e”。

-t 显示 TCP协议的连接情况。

-u 显示 UDP协议的连接情况。

-v 显示正在进行的工作。

例题 3 答案

（3）D

例题 4

在 SNMP 的网络管理者——网管代理模型中，__（4）__负责管理指令的执行。

（4）A．网络管理者　　B．网管代理　　C．网络管理协议　　D．管理信息库

例题 4 分析

SNMP 是一组协议标准，它主要包括管理信息库（MIB）、管理信息结构（SMI）和管理通信协议（SNMP）三个部分。其网络管理模型则是由管理进程（Manager，处于管理模型核心，负责完成网管各项功能）、代理（Agent，运行在设备上的管理程序，负责收集信息、管理指令的执行）、管理信息库三个部分组成的。

例题 4 答案

（4）B

例题 5

在 Windows 系统中，如果要查找到达目标主机 Csai 的网络路径，则应该键入的命令是__（5）__。

（5）A．traceroute Csai　　B．route Csai

C．tracert Csai　　D．net session Csai

例题 5 分析

在 Windows 操作系统中，可以使用 tracert 查找到达目标主机之间的网络路径，而在 UNIX 系统中等价的命令是 traceroute；而 route 命令是用来显示路由表的；net 命令是一个强大的网络工具命令，它有许多选项，其中 session 是用来列出当前的网络会话。

例题 5 答案

（5）C

例题 6

下列 SNMP 消息中，不属于 SNMPv1 的是__（6）__。

（6）A. GetRequet　　B. SetRequest

C. GetBulkRequest　　D. Trap

例题 6 分析

SNMPv2 中增加了两种 PDU，即 GetBulkRe-quest-PDU 和 InformRequest-PDU。GetBulkRequest-PDU 能在一次报文交换中，取回大批量的数据（如一次取回表中的多行数据）；在检索大量的管理信息时，它还能将交换的报文数量减到最少。GetBulkRequest-PDU 请求与 GetNextRequest 一样，是变量的下一个变量的取值。

例题 6 答案

（6）C

例题 7

网络管理的主要功能是配置管理、性能管理、计费管理、故障管理和安全管理，主要的网络管理协议有__（7）__，这两个协议分别涉及 OSI 模型的__（8）__。

（7）A．SNMP 和 CMIP　　B．SNMP 和 SMTP
　　C．CMIP 和 SMTP　　D．SMTP 和 HTTP

（8）A．下 3 层和上 4 层　　B．下 3 层和所有 7 层
　　C．下 2 层和上 5 层　　D．下 4 层和所有 7 层

例题 7 分析

CMIP 是公共管理信息协议，它是 OSI 提供的网络管理协议；SNMP 是简单网络管理协议，是应用最广泛的网络管理协议；SMTP 是简单邮件传输协议，与网络管理无关；HTTP 则是超文本传输协议，用于 Web 应用。这两个协议分别涉及了下三层和所有的七层。

例题 7 答案

（7）A　　（8）B

第 6 章　网络安全基础

随着计算机网络的飞速发展，网络中的安全问题也日趋严重，黑客攻击、信息泄密及病毒泛滥所带来的危害引起了世界各国尤其是信息发达国家的高度重视。

根据网络管理员的考试大纲要求，本章应掌握信息系统安全基础知识，网络安全漏洞、网络安全控制技术、网络防病毒系统等相关知识。本章的试题大约占 6 分，占上午考试的 8%左右。

6.1　网络安全基础概述

本知识点在于理解安全的基本要素、主要的安全威胁与可采取的安全措施，以及常见的安全技术。

6.1.1　网络安全的基本要素

计算机网络安全的五个基本要素为：

（1）机密性：确保信息不暴露给未授权的实体或进程。

（2）完整性：只有得到允许的人才能够修改数据，并能够判别数据是否已被篡改。

（3）可用性：得到授权的实体在需要时可访问数据。

（4）可控性：可以控制授权范围内的信息流向和行为方式。

（5）可审查性：对出现的安全问题提供调查的依据和手段。

而对于网络及网络交易而言，信息安全的基本需求是机密性（又称为保证性）、完整性和不可抵赖性（也就是数据发送、交易发送方无法否认曾经的事实）。

6.1.2　网络面临的安全性威胁

计算机网络上的通信面临以下的四种威胁：

（1）截获：攻击者从网络上窃听他人的通信内容。

（2）中断：攻击者有意中断他人在网络上的通信。

（3）篡改：攻击者故意篡改网络上传送的报文。

（4）伪造：攻击者伪造信息在网络上传送。

上述四种威胁可划分为两大类，即被动攻击和主动攻击。在上述情况中，截获信息的攻击称为被动攻击，而中断、篡改和伪造信息的攻击称为主动攻击。

在被动攻击中，攻击者只是观察和分析某一个协议数据单元 PDU 而不干扰信息流。

而在主动攻击中，攻击者对某个连接中通过的 PDU 进行各种处理，包括更改、删除、复制、记录、延迟等等。

对于被动攻击，通常很难被检测出来。对付被动攻击可采用各种数据加密技术。对于主动攻击，可以采取适当措施加以检测。对付主动攻击，则需将加密技术与适当的鉴别技术相结合。

6.1.3　计算机系统安全等级

根据美国国防部和国家标准局的《可信计算机系统评测标准》，可将系统分成四类 7 级：

（1）D 级：最低级别，保护措施小，没有安全功能。

（2）C 级：自定义保护级。安全特点是系统的对象可由系统的主题自定义访问权。

C1 级：自主安全保护级，能够实现对用户和数据的分离，进行自主存取控制，数据保护以用户组为单位。

C2 级：受控访问级，实现了更细粒度的自主访问控制，通过登录规程、审计安全性相关事件以隔离资源。

（3）B 级：强制式保护级。其安全特点在于由系统强制的安全保护。

B1 级：标记安全保护级。对系统的数据进行标记，并对标记的主体和客体实施强制存取控制。

B2 级：结构化安全保护级。建立形式化的安全策略模型，并对系统内的所有主体和客体实施自主访问和强制访问控制。

B3 级：安全域。能够满足访问监控器的要求，提供系统恢复过程。

（4）A 级：可验证之保护。

A1 级：与 B3 级类似，但拥有正式的分析及数学方法。

而根据我国《计算机信息系统安全保护等级划分准则》标准规定了计算机系统安全保护能力的五个等级，其划分与前者类似即：

（1）第一级：用户自主保护级；计算机信息系统可信计算机通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。

（2）第二级：系统审计保护级；与用户自主保护级相比，本级的计算机信息系统可信计算实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

（3）第三级：安全标记保护级；计算机信息系统可信计算具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。

（4）第四级：结构化保护级；计算机信息系统可信计算建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。

（5）第五级：访问验证保护级；计算机信息系统可信计算满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

6.2 网络安全漏洞

目前计算机在全世界越来越普及，互联网也正在以前所未有的发展势头向前发展。与以前仅仅使用网络发送电子邮件不同的是由于电子商务的推动，在网络上传输的信息越来越重要，它包括了知识产权、产品信息、采购指令、人力资源数据及信息卡号码等。然而在另一方面，由于互联网在最初设计时未充分考虑安全方面的需求，使它在安全方面先天不足，存在许多安全方面的漏洞。

6.2.1 网络安全漏洞的基本概念

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

漏洞会影响到很大范围的软硬件设备，包括操作系统本身及其支持软件，网络客户和服务器软件，网络路由器和安全防火墙等。换而言之，在这些不同的软硬件设备中都可能存在不同的安全漏洞问题。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

安全漏洞问题在一定程度上是独立于操作系统本身的理论安全级别而存在的。并不是说系统所属的安全级别越高，该系统中存在的安全漏洞就越少。但是可以这么理解，当系统中存在的某些漏洞被入侵者利用，使入侵者得以绕过系统中的一部分安全机制并获得对系统一定程度的访问权限后，在安全性较高的系统中，入侵者如果希望进一步获得特权或对系统造成较大的破坏，必须要克服更大的障碍。

6.2.2　网络安全漏洞的分类

每个系统都有漏洞，不论你在系统安全性上投入多少财力，攻击者仍然可以发现一些可利用的特征和配置缺陷。但现实中大多数攻击者所利用的都是常见的漏洞，因此我们应能在这些漏洞被利用之前查出网络的薄弱之处防患于未然。

网络安全漏洞大体上可以分为以下几类：

1）软件或协议编写错误造成的漏洞

协议是定义网络上计算机会话和通信的规则，如果协议的设计存在错漏，那么无论运用该协议的应用服务设计得多完美，它仍然是存在漏洞的。如在 TCP/IP 上发现了 100 多种安全弱点或漏洞。如 IP 地址欺骗、TCP 序号袭击、ICMP 袭击、IP 碎片袭击和 UDP 欺骗等等。另外软件的设计过程中往往存在着不全面的现象，如没有进行数据内容大小的检查；不能正常处理资源耗尽的情况；对运行环境没有做完整性的检查等。攻击者只要掌握了程序的惯用方法，通过渗透这些漏洞不需要特权账号就能获得额外的、未经授权的访问。计算机系统的使用不会是单纯的系统应用，新的软件、新的组件不断地添加到操作系统中，也就不断地为系统增加不可知的漏洞威胁了。

2）软件或协议实现造成的漏洞

有时候即使协议设计好了，但在实现协议的过程中仍可能引入漏洞。如邮件协议的一个实现中能够让攻击者通过与受害主机的邮件端口建立连接，达到欺骗受害主机执行非法任务的目的，或者是使入侵者具有了访问受保护文件和执行服务程序的权限。这样的漏洞往往导致了攻击者不需要访问主机的凭证就能够从远端控制服务器。

3）系统和网路配置不当造成的漏洞

这一类漏洞并不是由协议或软件本身造成的，而是由于它未能被正确地部署和配置造成的。通常在软件安装时都会有默认的配置，如果管理员不更改这些配置，服务器仍然能提供正常的服务，但是入侵者就能够利用这些配置对服务器进行攻击。如 FTP 服务器的匿名账号就曾为不少的管理员带来了麻烦。

6.2.3　网络安全漏洞的等级

一般来说漏洞的威胁类型基本上决定了它的严重性，根据漏洞所造成的影响和危害程度，我们可以把严重性分成高、中、低三个级别。远程和本地管理员权限应该对应为高，普通用户权限、权限提升、读取受限文件、远程和本地拒绝服务对应中级，远程非授权文件存取，口令恢复、欺骗、服务器信息泄露对应低级别。但这只是最一般的情况，很多时候需要具体情况具体分析，如一个涉及到针对系统本身的远程拒绝服务漏洞，就应该是高级别。同样一个被广泛使用的软件如果存在弱口令问题，有口令恢复漏洞，也应该归为中高级别。

6.2.4　网络漏洞扫描技术

漏洞扫描技术是检测本地或远程系统安全脆弱性的一种安全技术，通过使用漏洞扫描器，系统管理员能够发现所维护的 Web 服务器的各种 TCP 端口的分配、提供的服务、Web 服务软件版本和这些服务及软件呈现在 Internet 上的安全漏洞。从而便于网络管理员对网络漏洞进行修补，保护网络的安全。

常规标准，可以将漏洞扫描器分为两种类型：网络漏洞扫描器和主机漏洞扫描器。网络漏洞扫描器是指基于 Internet 远程检测目标网络和主机系统漏洞的程序，如提供网络服务、后门程序、密码破解和阻断服务等的扫描测试。主机漏洞扫描器是指针对操作系统内部进行的扫描，如 UNIX、NT、Linux 系统日志文件分析，可以弥补网络型安全漏洞扫描器只从外面通过网络检查系统安全的不足。

6.3　网络安全控制技术

网络安全控制技术对于整个网络的安全有着重要的意义，下面来具体了解一下访问安全控制技术的基本概念、分类及实现。

6.3.1　访问控制的概念

机密性服务和完整性服务都需要实施访问控制。访问控制是确定来访实体是否有访问权限及实施访问权限的过程。被访问的数据，如文件、数据报文、分组数据包、数据帧等，统称客体。能访问或使用客体的活动实体称做主体，如用户以及作为用户代理的进程、作业或任务等。访问控制一般都是基于安全政策和安全模型的。Lampson 提出的访问矩阵（Access Matrix）是表示安全政策的最常用的访问控制安全模型。该矩阵中的列表示访问者，即主体；行表示被访问对象，即客体。访问者对访问对象的权限就存放在矩阵中对应的交叉点上。

为节省存储空间，实际系统通常并不直接采用矩阵，而是采用访问控制表或者权利表进行表示。前一种方法是按照行来存储矩阵，在对象服务器上存储着每个对象的授权访问者及其权限的一张表，也称访问控制表（Access Control List，ACL）。负责保护访问对象的程序称为引用监控器（Reference Monitor），它根据访问控制表的内容来判断是否给某个访问者授权某些访问权限。后一种方法则是按照列来处理矩阵，每个访问者存储有访问权利（capability）的表，该表包含了它能访问的特定对象和操作权限。引用监视器根据验证访问表提供的权力表和访问者的身份来决定是否授予访问者相应的操作权限。

6.3.2　访问控制的分类

根据能够控制的访问对象粒度可以将访问控制分为粗粒度（Coarse Grained）访问控

制、中粒度（Medium Grained）访问控制和细粒度访问控制。这里并没有严格定义的区分标准，但是人们通常认为能够控制到文件甚至记录对象的访问控制可以称为细粒度访问控制，而只能控制到主机对象的访问控制称为粗粒度访问控制。

目前很多计算机系统的安全都是采用 ACL 模型，分布式系统和网络系统也不例外，可见，ACL 模型是安全保密和完整性安全策略的基础。

源通信参与方是通信发起者和请求者，请求信息包含了对网络资源进行某种操作的请求；ACL 服务器通过引用监控器检查源通信方的请求内容并决定是否允许通过；访问对象是网络资源，如文件、设备或者 CPU 等。

6.3.3　访问控制的实现

在集中式系统中访问控制是很容易实现的，因为操作系统控制着所有访问对象并且管理所有进程，所有操作均在主机操作系统管理下进行。在分布式系统和网络环境中情况有些不同，首先是访问者和被访问对象不在一台主机上，它们之间的通信路径可能很长并且中间可能经过很多台主机，这些主机的可信赖程度是不同的。因此在进行身份认证时必须将远程用户和本地用户加以区分，在设置访问控制权限时也要区别对待。例如有些资源只允许用户在本地进行访问。其次是规模不同，网络系统的规模比集中式系统要大得多，因此不可能由单个主机来负责管理所有用户及他们的访问控制信息。必须有机制保证引用监视器与这些用户管理和访问控制信息管理的服务器之间安全地通信，这里涉及访问控制信息数据完整性和对访问控制服务器的认证协议等问题。

为了简化管理，访问者通常被分类成组、组织，设置访问控制时可以按组进行设定，这样就可以避免访问控制表过于庞大。例如某文件允许所有清华大学学生阅读，那么在访问控制表中将清华大学学生作为组来定义是合适的，否则就需要在 ACL 中添加一万多项，而且随时需要根据学生毕业、入学而修改。当然这需要身份认证系统提供分组管理的功能。

网络资源包括信息资源和服务资源。授权控制框架是对网络资源进行授权管理和访问控制的基本框架，它独立于各种应用系统，独立于各个安全子系统的授权管理系统，对网络资源实施统一管理，是网络资源管理的最主要的安全机制。授权控制框架可对各种应用服务进行授权管理，包括 WWW 应用、客户机/服务器应用、TCP/IP 应用、数据库应用、面向对象的分布系统应用 CORBA、报文队列 MQ 应用等标准应用对象。授权管理系统提供的基本服务是授权管理、管理和维护授权策略、对象映射、用户角色等，并且要有使用方便的管理界面，可以进行安全的远程管理。应用服务系统通过授权应用程序接口获取授权信息，实施用户对对象的访问控制。授权控制框架也应基于国际标准以保证它的互操作性。

6.4 网络防病毒系统

"计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。"

本知识点重点在于了解计算机病毒的特点、分类，熟悉常见的几种病毒特征、入侵方式等。

6.4.1 计算机病毒的分类

按照计算机病毒的特点及特性，计算机病毒的分类方法有许多种。因此，同一种病毒可能有多种不同的分法。最常见的分类方法是按照寄生方式和传染途径分类。计算机病毒按其寄生方式大致可分为两类：一是引导型病毒，二是文件型病毒。混合型病毒集两种病毒特性于一体。

引导型病毒会去改写（即一般所说的"感染"）磁盘上的引导扇区（Boot Sector）的内容，软盘或硬盘都有可能感染病毒。再不然就是改写硬盘上的分区表（FAT）。如果用已感染病毒的软盘来启动的话，则会感染硬盘。

文件型病毒主要以感染文件扩展名为.com、.exe 和.ovl 等可执行程序为主。它的安装必须借助于病毒的载体程序，即要运行病毒的载体程序，方能把文件型病毒引入内存。已感染病毒的文件执行速度会减缓，甚至完全无法执行。有些文件遭感染后，一执行就会遭到删除。

混合型病毒综合引导型和文件型病毒的特性，它的"性情"也就比引导型和文件型病毒更为"凶残"。此种病毒透过这两种方式来感染，更增加了病毒的传染性以及存活率。不管以哪种方式传染，只要中毒就会经开机或执行程序而感染其他的磁盘或文件，此种病毒也是最难查灭的。

6.4.2 计算机病毒的特征

传统意义上的计算机病毒一般具有以下几个特点：

1．破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响，凡是由软件手段能触及到计算机资源的地方均可能受到计算机病毒的破坏。轻者会降低计算机工作效率，占用系统资源，重者可导致系统崩溃。

根据病毒对计算机系统造成破坏的程度，我们可以把病毒分为良性病毒与恶性病毒。良性病毒可能只是干扰显示屏幕，显示一些乱码或无聊的语句，或者根本没有任何破坏动作，只是占用系统资源。这类病毒较多，如 GENP、小球、W-BOOT 等。恶性病毒则有明确的目的，它们破坏数据、删除文件、加密磁盘甚至格式化磁盘，有的恶性病

毒对数据造成不可挽回的破坏。这类病毒有 CIH、红色代码等。

2．隐蔽性

病毒程序大多夹在正常程序之中，很难被发现，它们通常附在正常程序中或磁盘较隐蔽的地方（也有个别的以隐含文件形式出现），这样做的目的是不让用户发现它的存在。如果不经过代码分析，我们很难区别病毒程序与正常程序。一般在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在很短的时间里传染大量程序。而且受到传染后，计算机系统通常仍能正常运行，使用户不会感到有任何异常。

大部分病毒程序具有很高的程序设计技巧、代码短小精悍，其目的就是为了隐蔽。病毒程序一般只有几百字节，而 PC 对文件的存取速度可达每秒几百 KB 以上，所以病毒程序在转瞬之间便可将这短短的几百字节附着到正常程序之中，非常不易被察觉。

3．潜伏性

大部分计算机病毒感染系统之后不会马上发作，可长期隐藏在系统中，只有在满足特定条件时才启动其破坏模块。例如 PETER-2 病毒在每年的 2 月 27 日会提三个问题，答错后会将硬盘加密。著名的“黑色星期五”病毒在逢 13 号的星期五发作。当然最令人难忘的是 26 日发作的 CIH 病毒。这些病毒在平时会隐藏得很好，只有在发作日才会显露出其破坏的本性。

4．传染性

计算机病毒的传染性是指病毒具有把自身复制到其他程序中的特性。计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒会在这台计算机上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，在与其他机器进行数据交换或通过网络接触，病毒会在整个网络中继续传染。

正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的。而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

随着计算机软件和网络技术的发展，在今天的网络时代，计算机病毒又有了很多新的特点，比如主动通过网络和邮件传播，变种多，具有病毒、蠕虫和黑客程序的功能。

6.4.3　常见的病毒攻击

本节介绍几种在网络管理员考试中经常考查到的常见的病毒攻击行为。

1．ARP 欺骗攻击

ARP 攻击就是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞，攻击者只要持续不断地发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP 地址和 MAC 地址对应条目，造成网络中断或中间人攻击。

ARP 攻击主要是存在于局域网网络中，局域网中若有一个人感染 ARP 木马，则感染该 ARP 木马的系统将会试图通过“ARP 欺骗”手段截获所在网络内其他计算机的通信信息，并因此造成网内其他计算机的通信故障。

防范 ARP 攻击最常用的方法就是做 IP 和 MAC 绑定，Windows 操作系统带有 ARP 命令程序，可以在 Windows 的命令提示符下用 ARP 命令来完成 ARP 绑定。具体的 ARP 命令及相关参数见表 6-1 所示。

表 6-1 ARP 命令及参数

参数	命令格式	命令描述
-A	arp –a	查看当前计算机上的 ARP 映射表。可以看到当前的 ARP 的映射关系是动态的还是静态的
-S	arp –s w.x.y.z aa-bb-cc-dd-ee-ff	添加静态 ARP 实现 ARP 绑定。其中 w.x.y.z 代表要绑定 IP 地址，aa-bb-cc-dd-ee-ff 代表其 MAC 地址
-D	arp –d InetAddr [IfaceAddr]	删除指定的 IP 地址项，此处的 InetAddr 代表 IP 地址，要删除所有项，请使用星号(*)通配符代替

2．冲击波病毒攻击

“冲击波”是一种利用Windows系统的RPC漏洞进行传播、随机发作、破坏力强的蠕虫病毒。它不需要通过电子邮件（或附件）来传播，更隐蔽，更不易察觉。它使用 IP 扫描技术来查找网络上操作系统为 Windows 2000/XP/2003 的计算机，一旦找到有漏洞的计算机，它就会利用 DCOM（分布式对象模型，一种能够使软件组件通过网络直接进行通信的协议）RPC 缓冲区漏洞植入病毒体以控制和攻击该系统。中毒症状有：系统资源紧张，应用程序运行速度异常；系统无故重启，或在弹出“系统关机”警告提示后自动重启等等；网络速度减慢，“DNS”和“IIS”服务遭到非法拒绝，用户不能正常浏览网页或收发电子邮件；不能复制粘贴；Word、Excel、PowerPoint 等软件无法正常运行。

3．震荡波病毒攻击

震荡波（Worm.Sasser）利用 Windows 平台的 Lsass 漏洞进行传播，中招后的系统将开启 128 个线程去攻击其他网上的用户。中毒症状：可造成机器运行缓慢、网络堵塞，并让系统不停地进行倒计时重启。其破坏程度有可能超过“冲击波”。

4．熊猫烧香病毒攻击

熊猫烧香病毒又称“武汉男生”，随后又化身为“金猪报喜”，它是一个感染型蠕虫病毒，用户计算机中毒后可能会出现蓝屏、频繁重启以及系统硬盘中数据文件被破坏等现象。同时，该病毒的某些变种可以通过局域网进行传播，进而感染局域网内所有计算机系统，最终导致企业局域网瘫痪，无法正常使用，它能感染系统中exe，com，pif，src，html，asp 等文件，它还能中止大量的反病毒软件进程并且会删除扩展名为 gho 的文件（gho 文件是系统备份工具GHOST的备份文件），使用户的系统备份文件丢失。被感染的用户系统中所有.exe 可执行文件全部被改成熊猫举着三根香的模样。

6.4.4　常见病毒攻击防范

1．用常识进行判断

绝不打开来历不明邮件的附件或我们并未预期接收到的附件。对看来可疑的邮件附件要自觉不予打开。千万不可受骗，即使附件看来好像是 jpg 文件。这是因为 Windows 允许用户在文件命名时使用多个后缀，而许多电子邮件程序只显示第一个后缀，例如，我们看到的邮件附件名称是 wantjob.jpg，而它的全名实际是 wangjob.jpg.vbs，打开这个附件意味着运行一个恶意的 VBScript 病毒。

2．安装防病毒产品并保证更新最新的病毒库

我们应该在重要的计算机上安装实时病毒监控软件，例如卡巴斯基、瑞星等软件。并且至少每周更新一次病毒库（现在的杀毒软件一般都支持在线升级），因为防病毒软件只有最新才最有效。

值得注意的是，当我们首次在计算机上安装防病毒软件时，一定要花费些时间对机器做一次彻底的病毒扫描，以确保它尚未受过病毒感染。领先的防病毒软件供应商现在都已将病毒扫描作为自动程序，当用户在首次安装产品时会自动执行。

3．不要从任何不可靠的渠道下载任何软件

我们最好不要使用重要的计算机去浏览一些个人网站，特别是一些黑客类或黄色网站，不要随意在小网站上下载软件。如果非得下载，我们应该对下载的软件在安装或运行前进行病毒扫描。

4．使用其他形式的文档

常见的宏病毒使用 Microsoft Office 的程序传播，减少使用这些文件类型的机会将降低病毒感染风险。尝试用 RichText 存储文件，这并不表明仅在文件名称中用 RTF 后缀，而是要在 Microsoft Word 中，用“另存为”指令，在对话框中选择 RichText 形式存储。尽管 Rich Text Format 依然可能含有内嵌的对象，但它本身不支持 Visual BasicMacros 或 JScript。

5．不要用共享的软盘安装软件，或者是复制共享的软盘

这是导致病毒从一台机器传播到另一台机器的方式。一般人都以为不要使用别人的磁盘，即可防毒，但是不要随便用别人的计算机也是非常重要的，否则有可能带一大堆病毒回家。在网络环境下，要尽量使用无盘工作站，不用或少用有软驱的工作站。工作站是网络的门户，只要把好这一关，就能有效地防止病毒入侵。

6．禁用 Windows Scripting Host

Windows Scripting Host（WSH）运行各种类型的文本，但基本都是 VBScript 或 JScript。许多病毒（例如 Bubbleboy 和 KAK.worm）使用 Windows Scripting Host，无需用户点击附件，就可自动打开一个被感染的附件。

7．使用基于客户端的防火墙或过滤措施

如果我们的计算机需要经常挂在互联网上，就非常有必要使用个人防火墙保护我们的文件或个人隐私，并可防止不速之客访问我们的系统。否则我们的个人信息甚至信用卡号码和其他密码都有可能被窃取。

8．记住一些典型文件的长度

我们可以记下一些典型文件（例如 Command.com）的长度，并定期进行对比，一旦发现异常，即有中毒的可能。中毒的程序，绝大部分会改变长度，所以记住一个常见程序的长度，有助于判定是否有病毒入侵系统，尤其是 Command.com 文件，该文件如果被病毒感染，我们的计算机系统将体无完肤。

9．重要资料，必须备份

资料是最重要的，程序损坏了可重新复制，甚至再买一份。但是自己的重要资料或文档，可能是几年的研究成果，也可能是公司的财务资料，如果某一天，因病毒的原因毁于一旦，那将是最惨重的事情，所以我们必须养成定期备份重要资料的习惯。

6.4.5 基于网络的防病毒系统

目前互联网已经成为病毒传播最大的来源，电子邮件和网络信息传递为病毒传播打开了高速的通道。网络化带来了病毒传染的高效率，而病毒传染的高效率也对防病毒产品提出了新的要求。

网络病毒的传播方式有：

（1）直接从工作站拷贝到服务器中。

（2）病毒先传染工作站，在工作站内存驻留，等运行网络内的程序时再传染给服务器。

（3）病毒先传染工作站，在工作站内存驻留，在运行时直接通过映像路径传染到服务器。

（4）如果远程工作站被病毒侵入，则病毒也可以通过通信中的数据交换进入网络服务器中。

基于网络系统的病毒防护体系主要包括以下策略：

（1）防病毒一定要实现全方位、多层次防毒。

（2）网关防毒是整个防毒的首要防线。

（3）没有管理的防毒系统是无效的防毒系统。

（4）服务是整体防毒系统中极为重要的一环。

网络防病毒系统组织形式有：

（1）系统中心统一管理。

（2）远程安装升级。

（3）一般客户端的防毒。

（4）防病毒过滤网关。

（5）硬件防病毒网关。

6.5　容灾系统

尽管网络管理员们一再小心谨慎，但还是不可避免会发生各种各样的灾难。在这里，灾难的定义主要是指自然的和人为的灾难，包括系统硬件、网络故障、机房断电，甚至火灾、地震等。会导致计算机硬件、数据、系统和服务都会遭到不同程度的破坏。容灾系统指的是通过特定的机制，能够在灾难损害发生以后，最大程度保障提供正当应用服务的计算机信息系统。

6.5.1　容灾的等级

大体上讲，容灾可以分为三个级别：数据级别、应用级别及业务级别。从对用户整个业务连续性的保障程度来看，它们的高可用级别也逐渐提高。

1）数据级别

数据级别容灾的关注点在于数据，即灾难发生后可以确保用户原有的数据不会丢失或者遭到破坏。

数据级容灾较为基础，其中较低级别的数据容灾方案仅需利用磁带库和管理软件就能实现数据异地备份，达到容灾的功效；而较高级的数据容灾方案则是依靠数据复制工具，例如卷复制软件，或者存储系统的硬件控制器，实现数据的远程复制。数据级别容灾是保障数据可用的最后底线，当数据丢失时能够保证应用系统可以重新得到所有数据。从这种意义上讲，数据备份属于该级别容灾，用户把重要的数据存放在磁带上，如果考虑到高级别的安全性还可以把磁带运送到远距离的地方保存，当灾难发生后把数据从磁带中获取。该级别灾难恢复时间较长，仍然存在风险，尽管用户原有数据没有丢失，但是应用会被中断，用户业务也被迫停止。这种方案花费较低，构建简单。

2）应用级别

对于业务应用繁多，并且系统需要保持 7×24 小时连续运行的企业来说，显然需要高级别的应用容灾系统来满足他们的需求。

应用级容灾是在数据级容灾的基础上，再把执行应用处理能力复制一份，也就是说在备份站点同样构建一套应用系统。应用级容灾系统能提供不间断的应用服务，让用户应用的服务请求能够透明地继续运行，而感受不到灾难的发生，保证信息系统提供的服务完整、可靠、安全。

一般来说，应用级容灾系统需要通过更多软件来实现，它可以使企业的多种应用在灾难发生时进行快速切换，确保业务的连续性。

3）业务级别

用户构建了数据级容灾和应用级容灾都是在 IT 范畴之内，然而对于正常业务而言，仅 IT 系统的保障还是不够的。用户需要构建最高级别的业务级别容灾。

业务级容灾的大部分内容是非 IT 系统，比如电话、办公地点等。因为当一场大的灾难发生时用户原有的办公场所都会受到破坏，用户除了需要原有的数据、原有的应用系统，更需要工作人员在一个备份的工作场所能够正常地开展业务。

6.5.2　容灾与备份的区别

从定义上看，备份是指用户为应用系统产生的重要数据（或者原有的重要数据信息）制作一份或者多份拷贝，以增强数据的安全性。因此备份与容灾所关注的对象有所不同，备份关心数据的安全，容灾关心业务应用的安全，我们可以把备份称做是“数据保护”，而容灾称做“业务应用保护”。备份最多表现为通过备份软件使用磁带机或者磁带库将数据进行拷贝，也有用户使用磁盘、光盘作为存储介质；容灾则表现为通过高可用方案将两个站点连接起来。

备份与容灾是存储领域两个极其重要的部分，二者有着紧密的联系。

首先，在备份与容灾中都有数据保护工作，备份大多采用磁带方式，性能低，成本低；容灾采用磁盘方式进行数据保护，数据随时在线，性能高，成本高；其次，备份是存储领域的一个基础，一个完整的容灾方案必然包括备份的部分；同时备份还是容灾方案的有效补充，因为容灾方案中的数据始终在线，因此存储有完全被破坏的可能，而备份提供了额外的一条防线，即使在线数据丢失也可以从备份数据中恢复。

6.6　例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 7 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

DoS 攻击的目的是__（1）__。

（1）A．获取合法用户的口令和账号

B．使计算机和网络无法提供正常的服务

C．远程控制别人的计算机

D．监听网络上传输的所有信息

例题 1 分析

DoS 是 Denial of Service 的简称，即拒绝服务，造成 DoS 的攻击行为被称为 DoS 攻击，其目的是使计算机或网络无法提供正常的服务。最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。带宽攻击指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求就无法通过。连通性攻击指用大量的连接请求冲

击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。

例题 1 答案

（1）B

例题 2

__（2）__主要包括网络模拟攻击、漏洞检测、报告服务进程、提取对象信息以及评测风险、提供安全建议和改进措施等功能。

（2）A. 访问控制技术　　B. 漏洞扫描技术

C. 入侵检测技术　　D. 统一威胁安全管理技术

例题 2 分析

漏洞检测和安全风险评估技术，因其可预知主体受攻击的可能性和具体的指证将要发生的行为和产生的后果，而受到网络安全业界的重视。这一技术的应用可帮助识别检测对象的系统资源，分析这一资源被攻击的可能指数，了解支撑系统本身的脆弱性，评估所有存在的安全风险。

网络漏洞扫描系统就是这一技术的实现，她包括了网络模拟攻击，漏洞检测，报告服务进程，提取对象信息，以及评测风险，提供安全建议和改进措施等功能，帮助用户控制可能发生的安全事件，最大可能的消除安全隐患。安全扫描系统具有强大的漏洞检测能力和检测效率，贴切用户需求的功能定义，灵活多样的检测方式，详尽的漏洞修补方案和友好的报表系统，为网络管理人员制定与合理安全防护策略提供依据。

例题 2 答案

（2）B

例题 3

在非授权的情况下使用 Sniffer 接收和截获网络上传输的信息，请问这种攻击方式属于__（3）__。

（3）A. 放置特洛伊木马程序　　B. DoS 攻击

C. 网络监听　　D. 网络欺骗

例题 3 分析

在网络中，当信息进行传播的时候，可以利用工具，将网络接口设置在监听的模式，便可将网络中正在传播的信息截获或者捕获到，从而进行攻击。网络监听在网络中的任何一个位置模式下都可实施进行。而黑客一般都是利用网络监听来截取用户口令。比如当有人占领了一台主机之后，那么他要再想将战果扩大到这个主机所在的整个局域网的话，监听往往是他们选择的捷径。

例题 3 答案

（3）C

例题 4

__（4）__不能减少用户计算机被攻击的可能性。

（4）A．选用比较长和复杂的用户登录口令 B．使用防病毒软件

C．尽量避免开放过多的网络服务 D．定期扫描系统硬盘碎片

例题 4 分析

选用复杂的登录密码、使用防病毒软件和减少网络开放的服务都是加强计算机安全的有效办法，可以减少被攻击的可能性。而定期扫描系统硬盘碎片可以提高系统性能，但此项与系统安全无关。

例题 4 答案

（4）D

例题 5

以下不属于网络安全控制技术的是__（5）__。

（5）A．防火墙技术 B．访问控制技术

C．入侵检测技术 D．差错控制技术

试题 5 分析

差错控制技术通常是指对通信链路中数据传输的差错进行控制、排除的技术，不属于网络安全的范畴。

例题 5 答案

（5）D

例题 6

在网络安全中，中断攻击者是通过破坏网络系统的资源来进行攻击，从而破坏了信息的__（6）__。窃取是对__（7）__的攻击。DoS 攻击了信息的__（8）__。

（6）A．可用性 B．保密性 C．完整性 D．真实性

（7）A．可用性 B．保密性 C．完整性 D．真实性

（8）A．可用性 B．保密性 C．完整性 D．真实性

试题 6 分析

中断攻击是指通过破坏网络系统的资源，从而使得用户无法正常访问这些信息，并使信息不可用，因此是破坏了信息的可用性。窃取是指以特殊的手段访问未授权的信息，因此它是使数据的保密性失效。而 DoS 是拒绝服务攻击，将使受攻击的系统无法处理正常用户的请求，因此也是破坏了信息的可用性。

例题 6 答案

（6）A （7）B （8）A

例题 7

__（9）__不能减少用户计算机被攻击的可能性。

（9）A．选用比较长和复杂的用户登录口令

B．使用防病毒软件

C．尽量避免开放过多的网络服务

D．定期扫描系统硬盘碎片

试题 7 分析

选用复杂的登录密码，使用防病毒软件和减少网络开放都是加强计算机安全的有效办法，可以减少被攻击的可能性。而定期扫描系统硬盘碎片可以提高系统性能，但此项与系统安全无关。

例题 7 答案

（9）D

第 7 章　标准化与知识产权

根据考试大纲，在标准化知识章节重点要求考生掌握标准化机构和常见的国内外 IT 标准等方面的知识。

在知识产权的方面，虽然考试大纲对考查范围并没有明确的规定，但从历次考试试题来看，希赛教育专家特别提示：考试主要考查著作权法、计算机软件保护条例等。从考查形式来看，主要考查一些行为是否违反某个法律条款。

7.1　标准化基础知识

标准化机构是指制定、发布和管理各种标准的国际组织、区域性组织、政府或非政府组织、行业组织等。不同的标准化机构，所制定标准的级别也不同。

7.1.1　标准化机构

目前世界上有许多个国际和区域性组织在制定标准或技术规则，其中最大的是国际标准化组织（ISO）、国际电工委员会（IEC）和国际电信联盟（ITU）。

在中国按照国务院授权，在国家质量监督检验检疫总局的管理下，国家标准化管理委员会（SAC）统一管理全国标准化工作。

1．国际标准化组织（ISO）

国际标准化组织（International Organization for Standardization，ISO）是目前世界上最大、最有权威性的国际标准化专门机构。1946 年 10 月 14 日至 26 日，中、英、美、法、苏等 25 个国家的 64 名代表集会于伦敦，正式表决通过建立国际标准化组织。1947 年 2 月 23 日，ISO 章程得到 15 个国家标准化机构的认可，国际标准化组织宣告正式成立，总部设在瑞士的日内瓦。ISO 是联合国经理事会的甲级咨询组织和贸发理事会综合级（即最高级）咨询组织。此外 ISO 还与 600 多个国际组织保持着协作关系。

国际标准化组织的目的和宗旨是："在全世界范围内促进标准化工作的发展，以便于国际物资交流和服务，并扩大在知识、科学、技术和经济方面的合作"。其主要活动是制定国际标准，协调世界范围的标准化工作，组织各成员国和技术委员会进行情报交流，以及与其他国际组织进行合作，共同研究有关标准化问题。

ISO 的组织机构包括全体大会、主要官员、成员团体、通信成员、捐助成员、政策发展委员会、理事会、ISO 中央秘书处、特别咨询组、技术管理局、标样委员会、技术咨询组、技术委员会等。

ISO 技术工作是高度分散的，分别由 2700 多个技术委员会（TC）、分技术委员会（SC）和工作组（WG）承担。在这些委员会中，世界范围内的工业界代表、研究机构、政府权威、消费团体和国际组织都作为对等合作者共同讨论全球的标准化问题。管理一个技术委员会的主要责任由一个 ISO 成员团体（诸如 AFNOR、ANSI、BSI、CSBTS、DIN、SIS 等）担任，该成员团体负责日常秘书工作。与 ISO 有联系的国际组织、政府或非政府组织都可参与工作。

2．国际电工委员会（IEC）

国际电工委员会（International Electromechanical Commission，IEC）成立于 1906 年，至今已有 90 多年的历史。该委员会是世界上成立最早的国际性电工标准化机构，负责有关电气工程和电子工程领域中的国际标准化工作。

IEC 的宗旨是，促进电气、电子工程领域中标准化及有关问题的国际合作，增进国际间的相互了解。为实现这一目的，IEC 出版包括国际标准在内的各种出版物，并希望各成员在本国条件允许的情况下，在本国的标准化工作中使用这些标准。目前 IEC 的工作领域已由单纯研究电气设备、电机的名词术语和功率等问题扩展到电子、电力、微电子及其应用、通信、视听、机器人、信息技术、新型医疗器械和核仪表等电工技术的各个方面。

IEC 每年要在世界各地召开 100 多次国际标准会议，世界各国的近 10 万名专家在参与 IEC 的标准制定、修订工作。IEC 现在有技术委员会（TC）89 个、分技术委员会（SC）88 个。IEC 标准的权威性是世界公认的。

3．国际电信联盟（ITU）

国际电信联盟（International Telecommunication Union，ITU）是联合国的一个专门机构，也是联合国机构中历史最长的一个国际组织。该组织诞生于 1865 年 5 月 17 日，是由法、德、俄等 20 个国家在巴黎会议为了顺利实现国际电报通信而成立的，当时称“国际电报联盟”。1932 年，70 个国家的代表在西班牙马德里召开会议，决议把“国际电报联盟”改名为“国际电信联盟”，这个名称一直沿用至今。1947 年在美国大西洋城召开国际电信联盟会议，经联合国同意，国际电信联盟成为联合国的一个专门机构。

为了适应电信科学技术发展的需要，国际电报联盟成立后，相继产生了 3 个咨询委员会。1924 年在巴黎成立了“国际电话咨询委员会（CCIF）”，1925 年在巴黎成立了“国际电报咨询委员会（CCIT）”，1927 年在华盛顿成立了“国际无线电咨询委员会（CCIR）”。1956 年，国际电话咨询委员会和国际电报咨询委员会合并成为“国际电报电话咨询委员会”，即 CCITT。1972 年 12 月，国际电信联盟在日内瓦召开了全权代表大会，通过了国际电信联盟的改革方案，国际电信联盟的实质性工作由三大部门承担，它们是：国际电信联盟标准化部门（ITU-T）、国际电信联盟无线电通信部门和国际电信联盟电信发展部门。其中电信标准化部门由原来的国际电报电话咨询委员会（CCITT）和国际无线电咨询委员会（CCIR）的标准化工作部门合并而成，主要职责是完成国际电信联盟有关电信

标准化的目标，使全世界的电信标准化。

4．国家标准化管理委员会（SAC）

国家标准化管理委员会（Standardization Administration of China，SAC）是国务院授权履行行政管理职能，统一管理全国标准化工作的主管机构。

根据国务院确定的职责范围，国家标准化管理委员会将担负起参与起草、修订国家标准化法律、法规的工作；拟订和贯彻执行国家标准化工作的方针、政策；拟订全国标准化管理规章，制定相关制度；组织实施标准化法律、法规和规章、制度；负责制定国家标准化事业发展规划；负责组织、协调和编制国家标准（含国家标准样品）的制定、修订计划；负责组织国家标准的制定、修订工作，负责国家标准的统一审查、批准、编号和发布；统一管理制定、修订国家标准的经费和标准研究、标准化专项经费；管理和指导标准化科技工作及有关的宣传、教育、培训工作；负责协调和管理全国标准化技术委员会的有关工作；协调和指导行业、地方标准化工作；负责行业标准和地方标准的备案工作；代表国家参加国际标准化组织（ISO）、国际电工委员会（IEC）和其他国际或区域性标准化组织，负责组织 ISO、IEC 中国国家委员会的工作；负责管理国内各部门、各地区参与国际或区域性标准化组织活动的工作；负责签定并执行标准化国际合作协议，审批和组织实施标准化国际合作与交流项目；负责参与与标准化业务相关的国际活动的审核工作；管理全国组织机构代码和商品条码工作；负责国家标准的宣传、贯彻和推广工作；监督国家标准的贯彻执行情况；管理全国标准化信息工作；在质检总局的统一安排和协调下，做好世界贸易组织技术性贸易壁垒协议（WTO/TBT 协议）执行中有关标准的通报和咨询工作。

国务院有关行政主管部门和有关行业协会也设有标准化管理机构，分工管理本部门本行业的标准化工作。例如全国信息技术标准化技术委员会分工管理信息技术方面的标准化工作。

各省、自治区、直辖市及市、县质量技术监督局统一管理本行政区域的标准化工作。国家标准化管理委员会对省、自治区、直辖市质量技术监督局的标准化工作实行业务领导。

7.1.2 标准的层次

根据制定机构和适用范围的不同，标准可分为若干个级别。

1．标准分级

根据《中华人民共和国标准化法》，国内标准分为国家标准、行业标准、地方标准和企业标准。在全球范围内，标准的分级方式并不统一，一般可分为国际标准、行业标准、区域标准、企业标准和项目标准等。

1）国际标准

国际标准是指由国际联合机构制定和公布，提供各国参考的标准。国际标准化组织

（ISO）、国际电工委员会（IEC）和国际电信联盟（ITU）制定的标准均为国际标准。此外被 ISO 认可、收入 KWIC 索引中的其他 25 个国际组织制定的标准，也视为国际标准。

2）国家标准

国家标准是指由政府或国家级的机构制定或批准，适用于全国范围的标准，如：

GB（或 GB/T）——中华人民共和国国家标准。《中华人民共和国标准化法》规定，“国家标准由国务院标准化行政主管部门制定”。目前，国家标准由国家标准化管理委员会制定，国家质量监督检验检疫总局批准和公布。

ANSI（American National Standards Institute）——美国国家标准协会标准。

FIPS-NBS（Federal Information Processing Standards，National Bureau of Standards）——美国国家标准局联邦信息处理标准。

BS（British Standard）——英国国家标准。

JIS（Japanese Industrial Standard）——日本工业标准。

3）行业标准

行业标准是指由行业机构、学术团体或国防机构制定，并适用于某个业务领域的标准，如：

IEEE（Institute of Electrical and Electronics Engineers）——美国电气和电子工程师学会标准。

GJB——中华人民共和国国家军用标准，由国防科学技术工业委员会批准，适合于国防部门和军队。

DOD-STD（Department Of Defense Standards）——美国国防部标准，适用于美国国防部门。

MIL-S（MILitary Standards）——美国军用标准，适用于美国军队内部。

根据《中华人民共和国标准化法》，国内的行业标准由国务院有关行政主管部门制定，并报国务院标准化行政主管部门备案。

4）区域标准

区域标准是指由区域性国际联合机构制定和公布，提供区域内各国参考和执行的标准，如欧盟标准。

5）地方标准

地方标准是指由地方行政主管部门制定，仅适用于本地的标准。

根据《中华人民共和国标准化法》，地方标准由省、自治区、直辖市标准化行政主管部门制定，并报国务院标准化行政主管部门和国务院有关行政主管部门备案。

6）企业标准

企业标准是指一些大型企业或机构，由于工作需要制定的适用于本企业或机构的标准。

根据《中华人民共和国标准化法》，国内企业的产品标准需报当地政府标准化行政

主管部门和有关行政主管部门备案。《GB/T 1 标准化工作导则》规定，企业标准以 Q 字开头。

目前，国外个别大型 IT 企业自定的某些标准已成为事实上的全球工业标准。

7）项目标准

项目标准是指由某一科研生产项目组织制定，且为该项任务专用的标准。

2．各级标准之间的关系

《中华人民共和国标准化法》明确规定了国家标准、行业标准、地方标准和企业标准之间的关系。

（1）对需要在全国范围内统一的技术要求，应当制定国家标准。

（2）对没有国家标准而又需要在全国某个行业范围内统一的技术要求，可以制定行业标准。在公布国家标准之后，该项行业标准即行废止。

（3）对没有国家标准和行业标准而又需要在省、自治区、直辖市范围内统一的工业产品的安全、卫生要求，可以制定地方标准。在公布国家标准或者行业标准之后，该项地方标准即行废止。

（4）企业生产的产品没有国家标准和行业标准的，应当制定企业标准，作为组织生产的依据。已有国家标准或者行业标准的，国家鼓励企业制定严于国家标准或者行业标准的企业标准，在企业内部适用。

《中华人民共和国标准化法》同时规定，“国家鼓励积极采用国际标准”，但并没有明确指出：当国家标准与国际标准不一致时，应当采用哪个标准。按照国际惯例，当一国产品在另一国销售时，应当优先适用销售地的国家标准。

3．强制性标准与推荐性标准

《中华人民共和国标准化法》规定：国家标准、行业标准分为强制性标准和推荐性标准。保障人体健康，人身、财产安全的标准和法律、行政法规规定强制执行的标准是强制性标准，其他标准是推荐性标准。省、自治区、直辖市标准化行政主管部门制定的工业产品的安全、卫生要求的地方标准，在本行政区域内是强制性标准。

强制性国家标准以 GB 开头，推荐性国家标准以 GB/T 开头。但应注意，此项规定并不适用于国家早期发布的标准，当时的国家标准统一以 GB 开头。

强制性标准可分为全文强制和条文强制两种形式：

（1）标准的全部技术内容需要强制时，为全文强制形式。此类标准必须在“前言”的第一段以黑体字写明：“本标准的全部技术内容为强制性”。

（2）标准中部分技术内容需要强制时，为条文强制形式。此类标准应根据具体情况选用最简洁的方式，在标准“前言”的第一段以黑体字写明其强制性条文和非强制性条文。

根据国家质量技术监督局[2000]36 号文件，强制性内容的范围包括：

（1）有关国家安全的技术要求。

（2）保障人体健康和人身、财产安全的要求。

（3）产品及产品生产、储运和使用中的安全、卫生、环境保护、电磁兼容等技术要求。

（4）工程建设的质量、安全、卫生、环境保护要求及国家需要控制的工程建设的其他要求。

（5）污染物排放限值和环境质量要求。

（6）保护动植物生命安全和健康的要求。

（7）防止欺骗、保护消费者利益的要求。

（8）国家需要控制的重要产品的技术要求。

《中华人民共和国标准化法》规定：强制性标准，必须执行。不符合强制性标准的产品，禁止生产、销售和进口。生产、销售、进口不符合强制性标准的产品的，由法律、行政法规规定的行政主管部门依法处理，法律、行政法规未作规定的，由工商行政管理部门没收产品和违法所得，并处罚款；造成严重后果构成犯罪的，对直接责任人员依法追究刑事责任。

推荐性标准，国家鼓励企业自愿采用。这类标准不具有强制性，任何单位均有权决定是否采用，主要通过经济手段或市场因素自行调节。违犯这类标准，不构成经济或法律方面的责任。但应当指出，推荐性标准一经接受并采用，或各方商定同意纳入经济合同中，就成为各方必须共同遵守的技术依据，具有法律上的约束性。

新中国成立以来，我国最初研制发布的强制性标准数量较多。20 世纪 90 年代后，为了适应国内经贸发展，并与国际标准化接轨，国家标准主管部门曾多次对强制性标准的有关规定进行调整，并对已有强制性标准进行反复的清理整顿，使强制性标准的数量得到适当控制。

7.2　软件知识产权保护

知识产权是指公民或法人等主体依据法律的规定，对其从事智力创作或创新活动所产生的知识产品所享有的专有权利，又称为“智力成果权”、“无形财产权”，主要包括发明专利、商标以及工业品外观设计等方面组成的工业产权和自然科学、社会科学以及文学、音乐、戏剧、绘画、雕塑、摄影和电影摄影等方面的作品组成的版权和工业产权两部分。

知识产权是指公民或法人等主体依据法律的规定，对其从事智力创作或创新活动所产生的知识产品所享有的专有权利，又称为“智力成果权”、“无形财产权”，主要包括发明专利、商标以及工业品外观设计等方面组成的工业产权和自然科学、社会科学以及文学、音乐、戏剧、绘画、雕塑、摄影和电影摄影等方面的作品组成的版权和工业产权两部分。

知识产权是一种无形财产，具有专有性、时间性、地域性等主要特点。

（1）专有性即独占性或垄断性，指除权利人同意或法律规定外，权利人以外的任何人不得享有或使用该项权利。这表明权利人独占或垄断的专有权利受严格保护，不受他人侵犯。因而，知识产权应该与人格权、财产权并立而自成一类。

（2）地域性指只在所确认和保护的地域内有效；即除签有国际公约或双边互惠协定外，经一国法律所保护的某项权利只在该国范围内发生法律效力。

（3）时间性指只在规定期限保护。即法律对各项权利的保护，都规定有一定的有效期，各国法律对保护期限的长短可能一致，也可能不完全相同，只有参加国际协定或进行国际申请时，才对某项权利有统一的保护期限。

除了上述三个特点外，知识产权还有些其他特点，比如知识产权属于绝对权，在某些方面类似于物权中的所有权，例如是对客体为直接支配的权利，可以使用、收益、处分以及为他种支配（但不发生占有问题）；具有排他性；具有移转性（包括继承）等。知识产权是受法律保护的，同时也是受法律限制的。知识产权虽然是私权，虽然法律也承认其具有排他的独占性，但因人的智力成果具有高度的公共性，与社会文化和产业的发展有密切关系，不宜为任何人长期独占，所以法律对知识产权规定了很多限制：

（1）从权利的发生说，法律为之规定了各种积极的和消极的条件以及公示的办法。例如专利权的发生须经申请、审查和批准，对授予专利权的发明、实用新型和外观设计规定有各种条件（专利法第 22 条、第 23 条），对某些事项不授予专利权（专利法第 25 条）。著作权虽没有申请、审查、注册这些限制，但也有著作权法第 3 条、第 5 条的限制。

（2）在权利的存续期上，法律都有特别规定。这一点是知识产权与所有权大不同的。

（3）权利人负有一定的使用或实施的义务。法律规定有强制许可或强制实施许可制度。对著作权，法律还规定了合理使用制度。

7.2.1 知识产权的主要内容

知识产权是指公民、法人或者其他组织在科学技术方面或文化艺术方面，对创造性的劳动所完成的智力成果依法享有的专有权利。其实质是把人类的智力成果作为财产来看待。它的客体是人的智力成果，权利主体对客体为独占，这一点类似物权中的所有权，权利人从知识产权取得的利益既有经济性质的，也有非经济性的，这两个方面是紧密结合在一起的。

知识产权包括工业产权和版权（在我国称为著作权）两部分。工业产权又包括专利、商标、商号等权，而著作权由自然科学、社会科学以及文学、音乐、戏剧、绘画、雕塑、摄影和电影摄影等方面的作品组成，是法律上规定的某一单位或个人对某项著作享有印刷出版和销售的权利，任何人要复制、翻译、改编或演出等均需要得到版权所有人的许可，否则就是对他人权利的侵权行为，要负法律责任的。

1．专利权

专利权与专利保护是指一项发明创造向国家专利局提出专利申请，经依法审查合格后，向专利申请人授予的在规定时间内对该项发明创造享有的专有权。发明创造被授予专利权后，专利权人对该项发明创造拥有独占权，任何单位和个人未经专利权人许可，都不得实施其专利，即不得为生产经营目的制造、使用、许诺销售、销售和进口其专利产品。未经专利权人许可，实施其专利即侵犯其专利权，引起纠纷的，由当事人协商解决；不愿协商或者协商不成的，专利权人或利害关系人可以向人民法院起诉，也可以请求管理专利工作的部门处理。专利保护采取司法和行政执法“两条途径、平行运作、司法保障”的保护模式。本地区行政保护采取巡回执法和联合执法的专利执法形式，集中力量，重点对群体侵权、反复侵权等严重扰乱专利法治环境的现象加大打击力度。

2．商标权

商标权是指商标主管机关依法授予商标所有人对其注册商标受国家法律保护的专有权。商标是用以区别商品和服务不同来源的商业性标志，由文字、图形、字母、数字、三维标志、颜色组合或者上述要素的组合构成。我国商标权的获得必须履行商标注册程序，而且实行申请在先原则。 商标是产业活动中的一种识别标志，所以商标权的作用主要在于维护产业活动中的秩序，与专利权的作用主要在于促进产业的发展不同。

3．商业秘密

未公开的信息即商业秘密包括技术密集和经营秘密，只要这个秘密没有公开过，用法律的话说，法律内容和精确的轮廓不能从公共渠道获得，第二是有价值的有用的，获得了这项技术秘密、经营秘密，能够取得经济利益或者是形成竞争优势。

7.2.2　知识产权法

知识产权法是调整因创造、使用智力成果而产生的，以及在确认、保护与行使智力成果所有人的知识产权的过程中，所发生的各种社会关系的法律规范之总称。我国有关知识产权保护的法律法规主要包括专利、商标、著作权、计算机软件保护、反不正当竞争等方面的内容，下面我们来介绍一下常用的法律。

1．著作权法

1）著作权的归属

著作权属于作者，本法另有规定的除外。创作作品的公民是作者。由法人或者其他组织主持，代表法人或者其他组织意志创作，并由法人或者其他组织承担责任的作品，法人或者其他组织视为作者。如无相反证明，在作品上署名的公民、法人或者其他组织为作者。

2）著作权的保护期

作者的署名权、修改权、保护作品完整权的保护期不受限制。公民的作品，其发表权、本法第十条第一款第（五）项至第（十七）项规定的权利的保护期为作者终生及其

死亡后五十年，截止于作者死亡后第五十年的 12 月 31 日；如果是合作作品，截止于最后死亡的作者死亡后第五十年的 12 月 31 日。

法人或者其他组织的作品、著作权（署名权除外）由法人或者其他组织享有的职务作品，其发表权、本法第十条第一款第（五）项至第（十七）项规定的权利的保护期为五十年，截止于作品首次发表后第五十年的 12 月 31 日，但作品自创作完成后五十年内未发表的，本法不再保护。

电影作品和以类似摄制电影的方法创作的作品、摄影作品，其发表权、本法第十条第一款第（五）项至第（十七）项规定的权利的保护期为五十年，截止于作品首次发表后第五十年的 12 月 31 日，但作品自创作完成后五十年内未发表的，本法不再保护。

3）著作权许可使用

使用他人作品应当同著作权人订立许可使用合同，本法规定可以不经许可的除外，许可使用合同和转让合同中著作权人未明确许可、转让的权利，未经著作权人同意，另一方当事人不得行使。使用作品的付酬标准可以由当事人约定，也可以按照国务院著作权行政管理部门会同有关部门制定的付酬标准支付报酬。当事人约定不明确的，按照国务院著作权行政管理部门会同有关部门制定的付酬标准支付报酬。出版者、表演者、录音录像制作者、广播电台、电视台等依照本法有关规定使用他人作品的，不得侵犯作者的署名权、修改权、保护作品完整权和获得报酬的权利。

2．专利权法

专利权是为保护发明创造专利权，鼓励发明创造，有利于发明创造的推广应用，促进科学技术进步和创新，适应社会主义现代化建设的需要而设立的。

1）授予专利权的条件

授予专利权的发明和实用新型，应当具备新颖性、创造性和实用性。新颖性，是指在申请日以前没有同样的发明或者实用新型在国内外出版物上公开发表过、在国内公开使用过或者以其他方式为公众所知，也没有同样的发明或者实用新型由他人向国务院专利行政部门提出过申请并且记载在申请日以后公布的专利申请文件中。创造性，是指同申请日以前已有的技术相比，该发明有突出的实质性特点和显著的进步，该实用新型有实质性特点和进步。实用性，是指该发明或者实用新型能够制造或者使用，并且能够产生积极效果。

2）专利权的期限、终止和无效

发明专利权的期限为二十年，实用新型专利权和外观设计专利权的期限为十年，均自申请日起计算。

还有很多关于产权法方面的知识，希望大家能自己去多了解。

7.3 例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 7 道例题，考生可认

真完成例题，体会例题分析，巩固所学知识。

例题 1

我国标准分为国家标准化、行业标准、地方标准和企业标准四类，__（1）__是企业标准的代号。

（1）A．GB　　B．QJ　　C．Q　　D．DB

例题 1 分析

根据《企业标准化管理办法》第十二条规定的企业标准的代号、编号方法如图 7-1 所示。

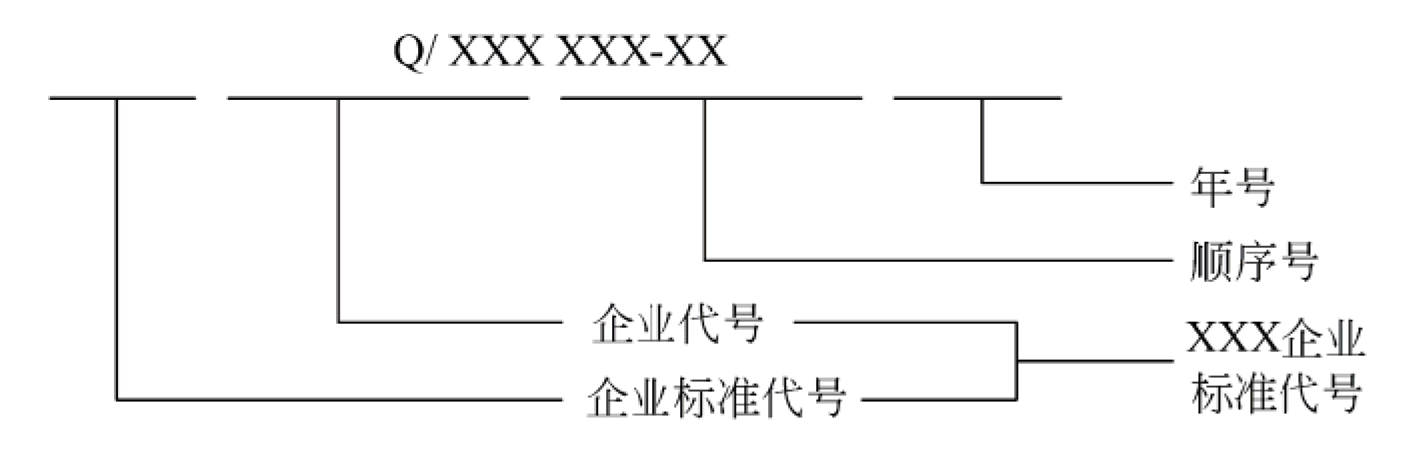


图 7-1　企业标准编码示意图

其中企业代号可用汉语拼音字母或阿拉伯数字或两者兼用组成。企业代号，按中央所属企业和地方企业分别由国务院有关行政主管部门和省、自治区、直辖市政府标准化行政主管部门会同同级有关行政主管部门规定。

例题 1 答案

（1）C

例题 2

__（2）__是关于质量管理体系的一系列标准，有助于企业交付符合用户质量要求的产品。

（2）A．ISO 9000　　B．CMM　　C．ISO 1400　　D．SW-CMM

例题 2 分析

ISO 9000 标准族是国际标准化组织中质量管理和质量保证技术委员会制定的一系列标准，现在共包括 20 个标准，如表 7-1 所示。

表 7-1　ISO 标准体系

① 质量术语标准		
ISO 8402		
④ 标准选用与实施指南	② 质量保证标准	③ 质量管理标准
ISO 9000	ISO 9001 设计、开发、生产、安装和服务	ISO 9004
–1 选择与使用	ISO 9002 生产、安装和服务	–1 指南
–2 实施	ISO 9003 最终检验和试验	–2 服务指南
–3 计算机软件		–3 流程性材料
–4 可信性大纲		–4 质量改进

续表

⑤ 支持性技术标准			
ISO 10005 质量计划 ISO 10007 技术状态	ISO 10011 –1 审核 –2 审核员 –3 审核管理	ISO 10012 –1 测量设备 –2 测量过程	ISO 10013 质量手册

例题 2 答案

（2）A

例题 3

GB/T 14394—93《计算机软件可靠性和可维护性管理》是__（3）__。

（3）A．推荐性国家标准　　B．强自性国家标准

C．指导性技术文件　　D．行业推荐性标准

例题 3 分析

我国国家标准的代号由大写汉语拼音组成，强制性国家标准代号为 GB，推荐性国家标准代号为 GB/T。行业标准代号由汉语拼音大写字母组成（如航天 QJ，电子 SJ，机械 JB、金融 JR），加上“/T”为推荐性标准，编号由主管部门申请，国务院标准化行政主管部门审查确定。地方标准代号由大写汉语拼音 DB 加上省级行政区划代码的前两位，加上“/T”一样说明为推荐性标准。企业标准代号由“Q/”加上企业代号组成。

因此，GB/T 14394—93《计算机软件可靠性和可维护管理》是推荐性国家标准。

例题 3 答案

（3）A

例题 4

小张在 M 公司担任程序员，他执行本公司工作任务，独立完成了某应用程序的开发和设计，那么该应用程序的软件著作权应当归属__（4）__享有。

（4）A．小张　　B．M 公司

C．M 公司和小张共同　　D．购买此应用程序的用户

例题 4 分析

根据《计算机软件保护条例》的规定，属于本职工作中明确规定的开发目标的软件作品属于职务软件，其著作权应归属公司所有。

例题 4 答案

（4）B

例题 5

著作权法中，计算机软件著作权保护的对象是__（5）__。

（5）A．硬件设备驱动程序　　B．计算机程序及其开发文档

C．操作系统软件　　D．源程序代码

例题 5 分析

根据《计算机软件保护条例》的规定，软件著作权保护的对象是计算机程序及开发文档，对其算法和用户界面是不作保护的。

例题 5 答案

（5）B

例题 6

甲委托乙开发一应用软件，如果双方并没有订立任何书面合同，那么该软件著作权应由__（6）__。

（6）A．乙一人享有　　B．甲、乙共同享有

C．甲一人享有　　D．甲、乙均不享有

例题 6 分析

依据《计算机软件保护条例》的第十一条之规定：接受他人委托开发的软件，其著作权的归属由委托人与受托人签订书面合同约定；无书面合同或者合同未作明确约定的，其著作权由受托人享有。

本题中，甲委托乙开发一应用软件，由于双方没有订立任何书面合同，所以该软件著作权由受托人乙一人享有。

例题 6 答案

（6）A

例题 7

商标法主要是保护__（7）__的权利。

（7）A．商标设计人　B．商标注册人　C．商标使用人　D．商品生产者

例题 7 分析

我国《商标法》第三条规定："经商标局核准注册的商标为注册商标，商标注册人享有商标专用权，受法律保护。"

例题 7 答案

（7）B

第 8 章　信息化基础

根据考试大纲的要求，本章要求考生理解信息化建设的基础知识，包括信息化的定义、全球信息化趋势，国家信息化战略，企业信息化战略和策略常识以及相关法律法规等等。

8.1　信息化的概念

所谓信息化，可以认为是现代信息技术与社会各个领域及其各个层面相互作用的动态过程及其结果。在这一相互作用过程中，信息技术自身和整个社会都发生着质的变化。其中社会的质的变化主要表现为信息资源开发和应用以及知识生产力迅速提高的结果。信息化是与当代信息革命、信息社会相关联的，信息化不同于工业化，工业化是信息化的基础，信息化可以促进工业化的进程；信息化不等同于现代化，在现代的时代背景下，信息化是现代化的目标之一；信息化不等于自动化，传统的自动化设备是以物质能源来驱动的，而对于信息化设备而言，信息不仅是处理对象，而且是信息系统的资源。

从本质上看，信息化应该是以信息资源开发利用为核心，以网络技术、通信技术等高科技技术为依托的一种新技术扩散的过程。作为这一过程的结果，它将最终会引起整个产业结构的变化，进而引起经济结构和社会结构的变化。

8.1.1　信息化的要素

信息化是一个非常广泛的和宏观的概念，而当人们谈到信息化时却总是具体的和有针对性的。关于信息化的内容，一般来说总是针对性非常强的。几年前，我国国家信息化管理部门列出了国家信息化体系的 6 个要素，可以作为区域信息化、行业信息化、企业信息化等的参考。

一是信息资源。信息和材料、能源共同构成经济和社会发展的三大战略资源。我国信息资源极其丰富，但开发利用的程度较低，远远落后于需要。因此开发和利用信息资源是我国信息化的关键一环和决定性的一环。

二是信息网络。信息网络是信息资源开发、利用的基础设施，信息网络包括计算机网络、电信网、电视网等。信息网络在国家信息化的过程中将逐步实现三网融合，并最终做到三网合一。

三是信息技术应用。信息技术应用是国家信息化中十分重要的要素，它直接反映了效率、效果和效益。

四是信息产业。信息产业是信息化的物质基础。信息产业包括微电子、计算机、电信等产品和技术的开发、生产、销售，以及软件、信息系统开发和电子商务等。从根本上来说，国家信息化只有在产品和技术方面拥有雄厚的自主知识产权，才能提高综合国力。

五是信息化人才。人才是信息化的成功之本，而合理的人才结构更是信息化人才的核心和关键。合理的信息化人才结构要求不仅要有各个层次的信息化技术人才，还要有精干的信息化管理人才、营销人才，法律、法规和情报人才。在信息化人才中有一种人才最为重要，那就是系统分析师。系统分析师既是信息化的技术人才，同时，又是经营管理人才，是一种复合型人才。而 CIO（首席信息官）又是系统分析师队伍的领军人物，是企业最高管理层的重要成员。

六是信息化政策、法规、标准和规范。信息化政策和法规、标准、规范是国家信息化快速、有序、健康和持续发展的保障。

8.1.2　信息化的意义

信息化的意义可以归结为以下三点：

1）促进组织创新

一个组织的结构如何，怎么进行运作往往是由信息的获取、处理、存储和传递的方式、手段和效率决定的。比如古代信息传递手段落后，用烽火台、信使、旗语、飞鸽传书等，这就决定了古代军队的组织形式和作战方式。而到了现在，由于信息技术异常发达，并被广泛地运用于战争，因而军队的组织形式和作战方式都发生了翻天覆地的变化，出现了信息化部队，以及立体战和信息战。对于企业或政府机构，由于信息技术和网络技术的广泛应用，使得它们才有可能大大缩减中间层，实现组织的扁平化。由于信息化引发的组织创新到处可见，比如虚拟企业、虚拟社区等。

2）促进管理创新

提高组织的管理水平除了学习管理知识、建立正确的管理理念外，更需要与之相匹配的管理手段。管理手段的提升会带动管理思想的转变，管理思想的转变反过来会对管理手段提出更高的要求，从而形成一个良性循环。

目前管理手段的信息化正是提升组织的管理水平的一条必由之路。尽管对于不同的组织来说，组织信息化的内容会有所不同，但是在应用信息技术、开发信息资源、培养信息人才等方面却是大体相同的。比如企业应用 ERP、CRM 等信息化管理软件，政府实施电子政务，建立电子政府，社会团体建立电子社区等，都能够大大提升管理水平。

3）促进经营创新

任何形式的组织（政府、军队、企业、社团）都毫不例外地生存于市场竞争的大环境里，都不可避免地要面对优胜劣汰的激烈竞争，只不过是竞争的表现形式和内容有所不同罢了。对于政府来说，就是要以最小的支出向社会提供最好的服务；对于企业来说，

就是创造更大的经济效益和社会效益。组织的运作过程也是组织的经营过程。经营与管理既有联系又有区别。经营主要是应对组织的外部环境的种种变化，其目的是趋利避害使组织得以生存和发展；而管理主要是改善组织的内部环境，使之能够更好地进行经营。理论研究和组织的实际运作都证明，没有好的管理，组织的经营就不会有力量，也不会有前途；而脱离经营的管理是没有方向和动力的管理，必然是无效的管理。之所以以前许多组织很容易把经营和管理分离开来，最主要的原因就是用传统的手段获取信息的渠道少，处理信息的效率非常低。而在信息化的环境下，比较易于做到把经营和管理融为一体，不断做到经营创新，从而提高组织的核心竞争力。

8.2 信息化的应用

现在，在高新技术产业发展和新经济兴起的过程中，信息技术及产业的发展是重要的核心和基础。信息产业的自身发展及信息技术的应用，推动了全球的经济增长和通货膨胀的降低，促进全球商业市场的形成。全球化的过程正是信息化的过程，信息化已经变得非常重要，受到了各企业、国家的重视。下面来分别介绍一下全球信息化趋势、我国信息化战略及企业信息化策略。

8.2.1 全球信息化趋势

从 20 世纪 90 年代初开始，全球信息化建设进入高潮。从那时起，各发达国家和发展中国家纷纷把信息作为一种战略资源加以对待，把信息化作为持续发展的重要途径。概括起来，全球信息化有以下表现和特点：

1）全球信息基础设施

信息基础设施是信息化的关键和基础，它决定了信息化的速度和质量，决定了信息资源开发利用的程度，进而决定了一个国家的经济发展水平和国际竞争力，因而信息基础设施建设成为全球信息化的重要特征和主要内容。

美国是信息技术大国，在世界信息产业发展的过程中一直处于主导地位。美国从自身的利益出发，积极倡导全球信息基础设施（俗称“全球信息高速公路”）建设。1994 年 9 月，前美国副总统戈尔提出建立全球信息基础设施（GII）的倡议。建议将各国的信息基础设施联结起来，组成世界信息高速公路，实现全球信息共享。还建议由世界银行帮助发展中国家解决资金困难，美国可为他们培训专业人员。

GII 对于加强国际经济和科学技术合作具有重要意义，尽管许多国家对信息高速公路建设想法不尽相同，但看到谁拥有信息，谁就拥有未来，对国家信息高速公路建设的重要性也就有了共识，都在摩拳擦掌，迎接挑战。

1995 年 2 月 15 日，美国政府在国内大规模宣传计算机及其网络的重要性，普及计算机知识，唤起民众，避免因信息占有量少而形成新的社会差距的同时，正式提出《全

球信息基础合作议程》，呼吁各国加入全球信息基础设施建设。

2）因特网迅速发展和普及

毫无疑问，因特网是全球信息化的代表，在一定意义上说，因特网就是全球信息化的代名词，因此，因特网的发展和普及就代表了全球信息化的趋势和方向。近年来，因特网的增长可以用爆炸性来形容。1996 年因特网用户在全球还不足 4000 万，到了 2008 年就达到数十亿，这表明一个基于网络的虚拟社会正在出现，一个全球性的、巨大的商业市场正在形成。

3）数字化浪潮来势迅猛

在 20 世纪 90 年代，美国学者尼葛洛庞帝出版了具有广泛影响力的著作《数字化生存》。尼葛洛庞帝是美国麻省理工学院教授及媒体实验室的创办人，同时也是《连线》杂志的专栏作家。西方媒体推崇他为计算机和传播科技领域最具影响力的大师之一，1996 年 7 月被《时代》周刊列为当代最重要的未来科学家之一。

《数字化生存》描绘了数字科技为我们的生活、工作、教育和娱乐带来的各种冲击和其中值得深思的问题，是跨入数字化新世界的最佳指南。

尼葛洛庞帝曾预言：我们的世界即将进入“比特的时代”，也就是进入“数字化”时代。

当世界进入 21 世纪以来，全球信息化的发展趋势已经证明了尼葛洛庞帝的预言是正确的。因特网的飞速发展和普及，把人们许多梦想变成了现实，突破时空和地域的界限进行有效沟通早已经成为人们生活中的一部分。

在当今数字时代，许多与现实世界相对应的数字世界不断出现在人们的眼前，例如数字地球、数字城市、数字企业，以及数字媒体、数字图书馆、数字医院，甚至还出现了数字人体。

总之，一个数字化浪潮正在迅猛地发展。

8.2.2　国家信息化战略

2000 年 10 月中共中央《关于制定国民经济和社会发展第十个五年计划建议的说明》中指出，“发达国家是在实现工业化基础上进入信息化发展阶段的。新的历史机遇，是我们可以把工业化与信息化结合起来，以信息化带动工业化，发挥后发优势，实现生产力的跨越式发展。我们讲抓住机遇，很重要的就是要抓住信息化这个机遇。发展以电子信息技术为代表的高新技术产业，同时用高新技术和先进实用技术改造传统产业，努力提高工业的整体素质和国际竞争力，使信息化与工业化融为一体，互相促进，共同发展。要加强信息基础设施建设，大力提高信息技术水平。要在全社会广泛应用信息技术，提高计算机和网络的普及应用程度。政府行政管理、社会公共服务、企业生产经营都要运用数字化、网络化技术，努力提高国民经济和社会信息化水平。”

用信息化带动工业化是我国 21 世纪的一项重大战略举措。信息化是由计算机与互

联网生产工具的革命所引起的工业经济转向信息经济的一种社会经济过程。它包括信息技术的产业化、传统产业的信息化、政府信息化、企业信息化等内容。

1）大力发展信息产业

信息产业是国家信息化的基础和保障，同时信息产业又是国民经济的支柱。因此大力发展信息产业是国家信息化战略的非常重要的组成部分。信息产业包括信息设备制造、软件产业、信息加工与服务等。在需求的拉动下，信息产业以每年 15%，甚至 20%以上的速度迅速发展，这是其他传统产业所不可比拟的。另一方面，信息技术及网络通信技术对政府、企业，以及整个社会的渗透力和影响力越来越大，以至于不断地从根本上改变着人们的生产和生活方式，对其他传统产业起到了很大的拉动作用。

当前，我国发展信息产业具有很多有利条件。

一是后发成本优势。我国能够通过贸易、投资和技术转让，超越一些历史发展阶段，直接学习和利用发达国家已有经验和技术，享受“后发优势”。作为后来者，我们不需要花费巨资来从事研究与开发，大大减少开发过程的风险成本。网络技术为后来者开辟了“新大陆”并大大降低了后继者的进入成本。可以利用先行者的知识和经验，这些知识和经验对后来者来说，重要性不亚于对科学技术的引进和利用。此外国际贸易不仅使后来者扩大了销售市场，促进了国内生产规模的扩大和生产效率的提高，而且还能引进国外的先进技术、资金和科学的管理方法。因而我们可以在劳动力成本上具有比较优势，可以吸引先行者的资本和技术，从而有利于克服要素“瓶颈”。

二是我国信息市场潜力巨大。我国有 13 亿人口，有着数量巨大的企业和政府机构，因而信息产品和服务的市场潜力巨大，为信息产业的发展提供了广阔的空间。

三是有较好的信息基础设施。在过去的十几年中，全国信息基础设施投入巨大，建设了覆盖全国的通信网络，包括光纤、数字微波、卫星、程控交换、移动通信、互联网等多种技术手段，正在向新一代宽带多媒体信息网络推进。

四是有市场体制支撑。信息化离不开市场经济体制。随着改革的不断深化，我国的社会主义市场经济体制不断完善提高。通过改革，特别是一系列有利于信息化的制度创新，为信息产业的发展提供强大的动力。

2）传统产业信息化

从国外现实来看，发达国家在抓信息技术产业化的同时，大力推进传统产业的信息化。20 世纪 90 年代以来，发达国家一方面高速发展以信息产业为核心的高新技术产业；另一方面，加速利用信息技术对传统产业进行改造，使产业结构进一步高级化。

信息化与工业化是一种互动、互补关系，不是替代关系。信息化产生于工业化，信息化的发展又需借助于工业化的手段，两者相互作用，共同发展。信息化主导着新时期工业化的方向，使工业朝着高附加值化发展；工业化是信息化的基础，为信息化的发展提供物资、能源、资金、人才以及市场。信息产业是知识密集型产业，把信息化与工业化结合起来，有利于搞好劳动密集型产业、资本密集型产业、技术密集型产业和知识密

集型产业的合理搭配，优化我国产业结构。

从发展的趋势来看，信息技术赋予工业化以新的内涵。信息同其他两大资源——材料和能源一样，自身具有增值的作用。信息革命的伟大成果使信息收集、信息处理、信息存储、信息传递、信息分析、信息使用及交互式网络化的信息交换实现了便捷、大容量、高速度和低成本，这就赋予工业化以新的内涵。由于我国的工业化远未走完，如果抛弃工业化来实现信息化是不可能的。只有用信息化武装起来的自主和完整的工业体系，才能为信息化提供坚实的物质基础。信息技术会使工业化产生倍增效应。能否利用信息化推动工业化已经成为当代后发展国家实现工业化、现代化的关键。

用信息技术改造传统制造业。信息化包括信息的生产和应用两大方面：一是信息技术的产业化；二是传统产业的信息化：信息生产要求发展一系列高新信息技术及产业，既涉及微电子产品、通信器材和设施、计算机软硬件、网络设备的制造等领域，又涉及信息和数据的采集、处理、存储等领域。信息技术在经济领域的应用主要表现在用信息技术改造和提升农业、工业、服务业等传统产业上。

信息技术提升传统产业。信息技术有高度创新性、高度渗透性和高度倍增性。它能提高传统产业产品的科技含量，增加其附加值。如计算机辅助设计、计算机集成制造、机电一体化以及电子商务引发商务领域的变革等，成为推动产业升级的重要力量。信息技术对结构升级的作用是深入、立体和内在的提升，能够在其他产业的研发、生产、销售等所有环节发挥作用，提高技术水平，降低产品成本，增加产品附加值，实现产业升级。

信息技术能够促进传统产业的分化和替代。高新技术产业的发展将对传统产业造成巨大的冲击，并使传统产业不断走向分化，在分化过程中，有的被淘汰出局，有的实现了升级换代。通过信息化带动经济结构调整，促使我国经济增长方式从高投入、高消耗、低效益、低质量的粗放型增长转变为高速度、高效益、低投入、低消耗的节约型增长。信息产业因其关联度、感应度、带动度大，它能提供高技术、高性能的产品和服务，从而突破现有的需求约束，创造新的需求，带动新产业的发展。

信息技术突破了传统产业的时空限制。卫星通信、高速网络、可视电话、联机检索、电视会议系统等一系列先进技术使信息的流通时间大大缩短，从而加快了财富的增值过程。

3）政府信息化

政府信息化的主要内容是电子政务。关于电子政务，目前有很多种说法。例如，电子政府、网络政府、政府信息化管理等。真正的电子政务绝不是简单的“政府上网工程”，更不是为数不多的网页型网站系统。严格地说，所谓电子政务，就是政府机构应用现代信息和通信技术，将管理和服务通过网络技术进行集成，在互联网上实现政府组织结构和工作流程的优化重组，超越时间和空间及部门之间的分隔限制，向社会提供优质和全方位的、规范而透明的、符合国际水准的管理和服务。

电子政务是一个系统工程，应该符合三个基本条件：

第一，电子政务是必须借助于电子信息化硬件系统、数字网络技术和相关软件技术的综合服务系统；硬件部分：包括内部局域网、外部互联网、系统通信系统和专用线路等；软件部分：大型数据库管理系统、信息传输平台、权限管理平台、文件形成和审批上传系统、新闻发布系统、服务管理系统、政策法规发布系统、用户服务和管理系统、人事及档案管理系统、福利及住房公积金管理系统，等数十个系统。

第二，电子政务是处理与政府有关的公开事务，内部事务的综合系统。包括政府机关内部的行政事务以外，还包括立法、司法部门以及其他一些公共组织的管理事务，如检务、审务、社区事务等。

第三，电子政务是新型的、先进的、革命性的政务管理系统。电子政务并不是简单地将传统的政府管理事务原封不动地搬到互联网上，而是要对其进行组织结构的重组和业务流程的再造。因此，电子政府在管理方面与传统政府管理之间有显著的区别。

电子政务的内容非常广泛，国内外也有不同的内容规范，根据国家政府所规划的项目来看，电子政务主要包括这样几个方面：

- 政府间的电子政务：政府间的电子政务是上下级政府、不同地方政府、不同政府部门之间的电子政务。主要包括：电子法规政策系统、电子公文系统、电子司法档案系统、电子财政管理系统、电子办公系统、电子培训系统、业绩评价系统等。
- 政府对企业的电子政务：政府对企业的电子政务是指政府通过电子网络系统进行电子采购与招标，精简管理业务流程，快捷迅速地为企业提供各种信息服务。主要包括：电子采购与招标、电子税务、电子证照办理、信息咨询服务、中小企业电子服务等。
- 政府对公民的电子政务：政府对公民的电子政务是指政府通过电子网络系统为公民提供的各种服务。主要包括：教育培训服务、就业服务、电子医疗服务、社会保险网络服、公民信息服务、交通管理服务、公民电子税务、电子证件服务等。

4）企业信息化

信息化是一个含义十分广泛的概念，它包含政府信息化、区域信息化、产业信息化、社会信息化等。但是有一点是确定的，那就是信息化的重点和关键是企业信息化。因为企业是市场竞争的主体，是社会生产力的主体，也必然是信息化的主导力量。

8.2.3 企业信息化策略

企业信息化是指企业以业务流程的优化和重构为基础，在一定的深度和广度上利用计算机技术、网络技术和数据库技术，控制和集成化管理企业生产经营活动中的各种信息，实现企业内外部信息的共享和有效利用，以提高企业的经济效益和市场竞争力。

企业要应对全球化市场竞争的挑战，特别是大型企业要实现跨地区、跨行业、跨所有制、跨国经营的战略目标，要实施技术创新战略、管理创新战略和市场开拓战略，要将企业工作重点转向技术创新、管理创新和制度创新的方向上来，信息化是必然选择和

必要手段。企业信息化涉及到对企业管理理念的创新，管理流程的优化，管理团队的重组和管理手段的革新。

首先，技术创新。现实的情况是：一方面，我国企业能够拥有并掌握的技术创新成果甚少，相关信息闭塞。另一方面，又有大量的技术开发成果被沉淀和搁置，造成惊人的浪费。对此，必须运用信息技术，通过在生产工艺设计、产品设计中计算机辅助设计系统的应用，通过互联网及时了解和掌握创新的技术信息，才能加快技术向生产的转化。还有生产技术与信息技术相结合，能够大幅度地提高技术水平和产品的竞争力，比如信息技术与洗衣机生产相结合，就生产出了自动洗衣机，增加了附加价值。

第二，管理创新。管理是一门科学，管理创新必须学习和掌握科学的方法。按照市场发展的要求，要对企业现有的管理流程重新整合，从作为管理核心的财务、资金管理，转向技术、物资、人力资源的管理，并延伸到企业技术创新、工艺设计、产品设计、生产制造过程的管理，进而还要扩展到客户关系管理、供应链的管理乃至发展到电子商务。实现这样的管理目标，就必须借助信息技术，发挥计算机的信息采集、储存功能和网络的传递与共享功能。

第三，制度创新。在建立现代企业制度的过程中，信息化起着重要的作用。特别是在由计划经济体制向市场经济体制转轨的过程中，赋予企业信息化一系列特殊的使命，那些不适应企业信息化的管理体制、管理机制和管理制度必须得到创新。同时通过计算机网络系统管理，建立起明确的岗位责任和精准的监管体系；借助互联网获取更全面、系统、及时的信息，彻底改变企业一直沿用的计划经济的资源分配方式和管理方式，注重市场信息的分析和研究，提供准确及时的决策信息；应用科学的方法实施管理。因此建立在计算机网络技术基础上的管理，才更科学、更有效。我们在倡导企业技术改造、技术创新的同时，还应当倡导企业加快管理改造和管理创新。

8.3　互联网相关的法律法规知识

当前随着互联网的逐步普及，互联网与人们工作、生活的关系更加密切。与此同时，我国互联网的法制建设也与互联网同步进行。虽然我国的互联网法律体系还不完善，但它的基本框架已经初步形成。到目前为止，我国已经出台的互联网相关的法律、法规主要有 4 个方面：计算机信息网络管理、计算机网络安全管理、互联网域名管理、互联网信息服务管理等。

计算机信息网络管理的有关法律、法规是“调整国家对网络提供商，国家对最终用户的管理被管理的权利义务关系。在这两种关系中，双方的地位是不对等的，管理与被管理的关系具有强制性。”国家对于网络提供商、最终用户的管理主要是行政上的管理，也包括对某些刑事案件的管辖。

网络安全是所有网络信息使用行为得以正常进行的前提和基础，自从互联网引进我

国开始，我国的有关部门就给以极大的关注，并相继出台了一系列的法律和法规，从而保证了我国互联网的安全运行。

互联网域名管理是计算机信息网络管理中的一项特殊且重要的内容。在这方面，国家有关主管部门根据有关法律、法规出台了一系列的管理办法和规定，较好地规范了互联网有关域名注册和使用行为，其中重要的一点是中文域名的注册和使用。

互联网信息服务，是指通过互联网向上网用户提供信息的服务活动。为了规范互联网信息服务活动，国务院于2000年9月25日公布施行了《互联网信息服务管理办法》。

8.4 例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了4道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

从信息资源管理的观点出发，信息系统的逻辑结构一般由四部分组成，其中__（1）__利用信息系统提供的信息进行决策和选择，是信息系统服务的对象。

（1）A．信息源　B．信息处理器　C．信息使用者　D．信息管理者

例题 1 分析

信息系统的基本结构可以概括为四大部件，即信息源、信息处理器、信息使用者和信息管理者。此外MIS还包括计算机网络、数据库和现代化的管理等扩展部件，这些是MIS的三大支柱。

（1）信息源。即信息发生的来源，信息的产生地。信息源是指企业内部生产经营活动中所产生的各种数据，如生产数据、财务数据、销售数据等。

（2）信息处理器。完成数据的采集、数据变换和数据存储等，并将数据转变为信息提供给信息用户。

（3）信息使用者。是企业各不同部门和不同层次的管理人员。

（4）信息管理者。是指负责管理信息系统开发和运行的人员，并在系统实施过程中负责信息系统各部分的组织和协调。

例题 1 答案

（1）C

例题 2

信息系统开发的结构化方法中，一个主要原则是__（2）__。

（2）A．自顶向下原则　B．自底向上原则

C．整体推进原则　D．重点突破原则

例题 2 分析

在信息系统开发的结构化方法中，采用结构化技术（结构化分析、结构化设计和结

构化实现）来完成软件开发的各项任务。这种方法学把软件生命周期的全过程依次划分为若干个阶段，然后顺序地完成每个阶段的任务。

结构化分析（Structured Analysis，SA）方法是一种面向数据流的需求分析方法。它的基本思想是自顶向下逐层分解，把一个大问题分解成若干个小问题，每个小问题再分解成若干个更小的问题。经过逐层分解，每个最底层的问题都是足够简单、容易解决的，于是复杂的问题也就迎刃而解了。

结构化设计（Structured Design，SD）方法是一种面向数据流的设计方法，它是以结构化分析阶段所产生的文档（包括数据流图、数据字典和软件需求说明书）为基础，自顶向下，逐步求精和模块化的过程。结构化设计通常可分为概要设计和详细设计。概要设计的任务是确定软件系统的结构，进行模块划分，确定每个模块的功能、接口以及模块间的调用关系。详细设计的任务是为每个模块设计实现的细节。

结构化程序设计（Structured Programming，SP）采用自顶向下逐步求精的设计方法和单入口单出口的控制结构。在设计一个模块的实现算法时先考虑整体后考虑局部，先抽象后具体，通过逐步细化，最后得到详细的实现算法。单入口单出口的控制结构，使程序的静态结构和动态执行过程一致，具有良好的结构，增强了程序的可读性。

针对程序中大量无节制地使用 GOTO 语句导致程序结构混乱的现象，Dijkstra 于 1965 年提出在程序语言中取消 GOTO 语句。1966 年，Bohm 和 Jacopini 证明了任何单入口、单出口、没有死循环的程序都能用三种基本的控制结构来构造，这三种基本的控制结构是：顺序结构、IF_THEN_ELSE 型分支结构（选择结构）和 DO_WHILE 型循环结构。如果程序设计中只允许使用这三种基本的控制结构，则称为经典的结构化程序设计；如果还允许使用 DO_CASE 型多分支结构和 DO_UNTIL 型循环结构，则称为扩展的结构化程序设计；如果再加上允许使用 LEAVE（或 BREAK）结构，则称为修正的结构化程序设计。

例题 2 答案

（2）A

例题 3

企业实施全面信息化战略的考虑因素之一应是__（3）__。

（3）A．信息技术及产品的发展水平　　B．企业是否取得了明显的效益

C．企业是否招收了一批信息技术人员　　D．行业及竞争对手的信息化水平

例题 3 分析

在企业实施全面信息化战略时，要考虑的主要因素是行业及竞争对手的信息化水平。

例题 3 答案

（3）D

例题 4

以下选项中，主要联系高层管理人员的信息系统是__（4）__。

（4）A．MIS（管理信息系统）

B．DSS（决策支持系统）

C．EDPS（电子数据处理系统）

D．TPS（事务处理系统）

例题 4 分析

信息系统一般泛指收集、存储、处理和传播各种信息，具有完整功能的集合体。它一直以来都与计算机和网络技术同步发展，历经四个主要阶段，如表 8-1 所示。

表 8-1 信息系统类型

发展阶段	说明	示例
电子数据处理系统（EDPS）	简单数据处理，仅用于科学计算，较少涉及管理内容	计算工资、统计账目
事务处理系统（TPS）	对企业局部事务的管理	财会、销售、物资、生产管理
管理信息系统(MIS)	是用系统思想建立起来的，以电子计算为基本信息处理手段，以现代通信设备为基本传输工具，并且能为管理决策提供信息化服务的人机系统	集成了事务处理中的局部应用，形成全局性、整体性的计算机应用
决策支持系统（DSS）	为高层决策提供支持的系统	ERP（集成了 MIS）、SRM 等

例题 4 答案

（4）B

第 9 章　网络新技术

计算机技术发展日新月异，因此，网络管理员考试要求掌握一些最新的、比较成熟的计算机网络技术。

9.1　无线局域网

无线局域网提供了移动接入的功能，这就给很多需要发送数据但不能坐在办公室的工作人员提供了方便。当一个工厂跨越的面积很大时，若要把各个部门都用电缆连接成网，其费用可能很高。但如果采用无线局域网，不仅可以节省投资，而且建网的速度也会变快。另外如果当大量持有便携式计算机的用户都在同一个地方同时要求上网时，若用电缆连网，那么布线也将成为一个很大的问题，而采用无线局域网的方式烦恼将不复存在。

9.1.1　无线局域网概述

无线局域网（WLAN），它主要运用射频（Radio Frequency，RF）的技术取代原来局域网系统中必不可少的传输介质（如同轴电缆、双绞线等）来完成数据信号的传送任务。就应用层上提供的服务功能来说，它与有线局域网没什么不同之处。只是由于无线局域网的传输媒介不同（它是无线方式的），所以无论是在硬件架设、空间使用限制的弹性、使用的机动性、便利性等都要比传统的有线局域网有更多的优势。而且在网络建设的成本上，它还可以节省一笔非常可观的网络布线费用。

9.1.2　无线局域网的拓扑结构

无线局域网可分为两大类。分别是有接入点（Access Point，AP，访问点、基站）模式（基础设施网络）和无接入点模式（Ad hoc 网络）。其结构如图 9-1 所示。

1．基础设施网络

整个网络都使用无线通信的方式，但是系统中存在接入点（AP）这样的设备，通过 AP 把一组终端站点逻辑上联系在一起，形成一个局域网络系统。这种结构的模式在实际应用中比较广泛。AP 的作用与网桥类似，负责在 802.11 和 802.3 的 MAC 协议之间进行转换。一个接入点覆盖的部分称为一个基本业务域（BSA），而接入点控制的所有终端

组成一个基本业务集（BSS），由两个以上的 BSA 可以组成一个分布式系统（DS）。

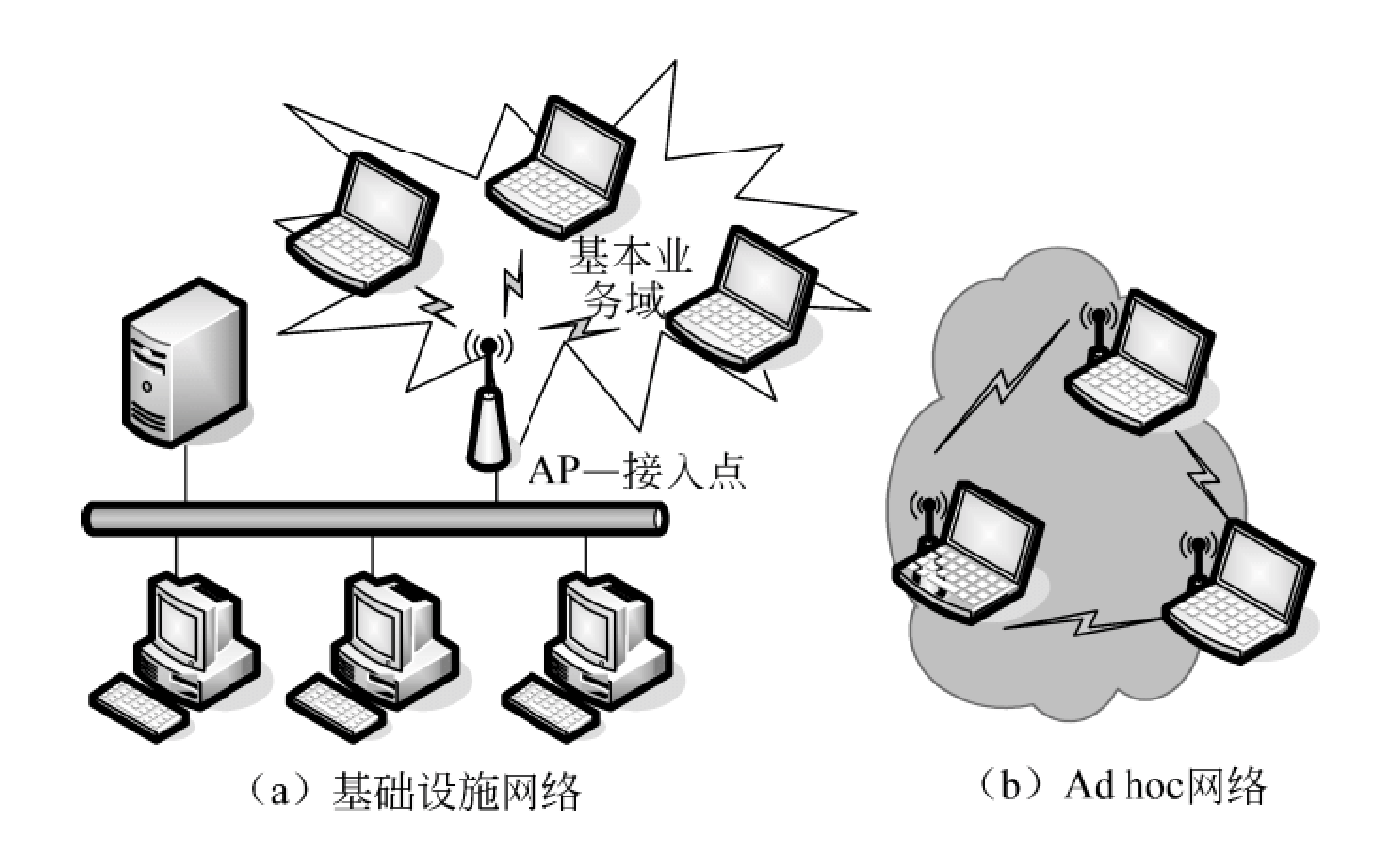


图 9-1　两种 WLAN 网络拓扑

2．Ad hoc 网络

整个网络都使用无线通信的方式，它也是一种特殊的无线网络应用模式。直接通过无线网卡实现点对点连接，实现资源共享。系统中并没有 AP 这样的设备，和基础设施网络相比，可扩展性和灵活性更好，但是路由、协调控制等技术都难以解决。

在大多数情况下，无线通信通常是作为有线通信的一种补充和扩展。在这种部署配置下，多个 AP 通过线缆连接在有线网络上，以使无线用户能够访问网络的各部分，如图 9-2 所示。

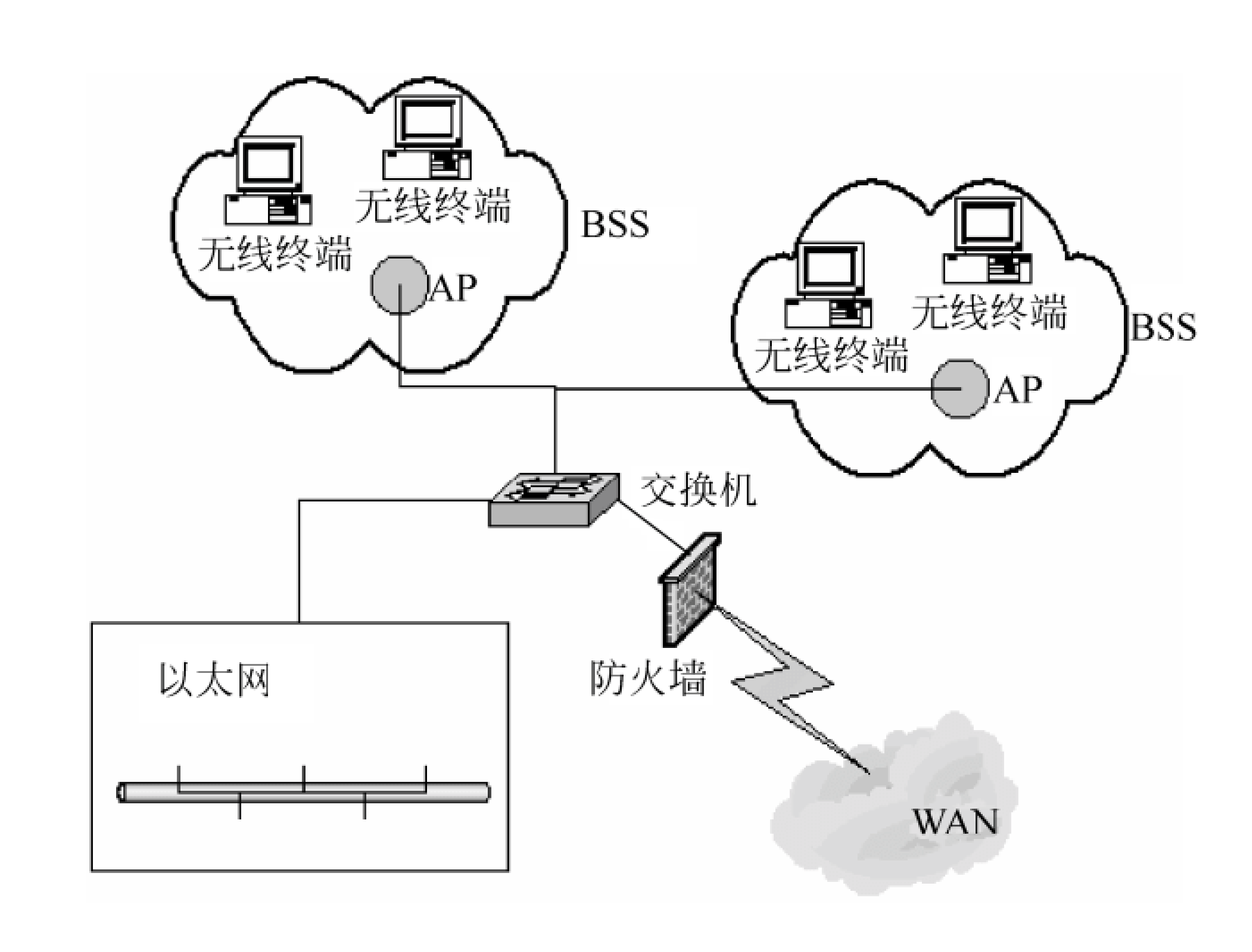


图 9-2　组合方式的 WLAN

9.1.3　IEEE 802.11 标准

IEEE 802 委员会为无线局域网开发了一组标准，即 IEEE 802.11 标准。虽然 IEEE 802.11 系列标准为建设无线局域网及开发与它相关的产品提供了技术上统一的依据和口径，但是这里需要补充说明的是，目前市场上并不是所有的与无线局域网络相关的产品都采用或符合这个标准。

1．无线局域网（WLAN）的基本模型

图 9-3 是 IEEE 802.11 工作组开发的一个模型。无线局域网的最小构成模块是基本服务集（Basic Service Set，BSS），它由一些运行相同 MAC 协议和争用同一共享介质的站点组成。基本服务集可以是单独的，也可以通过网络接入点连到骨干分布系统。网络接入点的作用类似于网桥。MAC 协议可以是完全分布式的，也可以由处于接入点的中央协调功能来完成。通常把 BSS 称为一个单元（cell）。

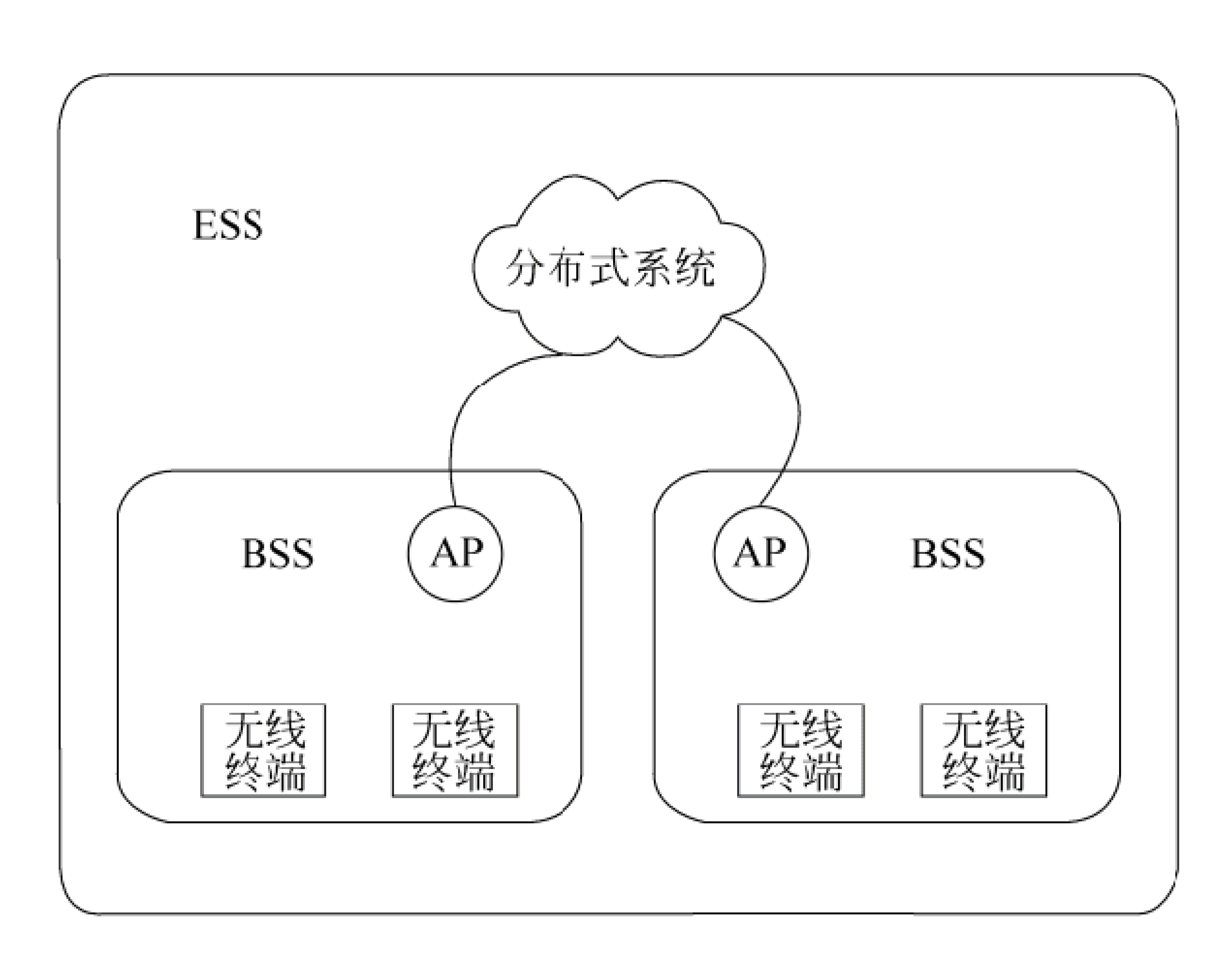


图 9-3　IEEE 802.11 工作组开发的一个模型

一个扩展服务集（Extended Service Set，ESS）由两个或更多的通过分布系统互连的 BSS 组成。一般分布系统是一个有线骨干 LAN。扩展服务集相对于逻辑链路控制层来说，只是一个简单的逻辑 LAN。

基于移动性，无限局域网标准定义了三种站点：

（1）不迁移。这种站点的位置是固定的或者只是在某一个 BSS 的通信站点的通信范围内移动。

（2）BSS 迁移。站点从某个 ESS 的 BSS 迁移到同一 ESS 的另一个 BSS。在这种情况下，为了把数据传输给站点，就需要具备寻址功能以便识别站点的新位置。

（3）ESS 迁移。站点从某个 ESS 的 BSS 迁移到另一 ESS 的一个 BSS。在这种情况下，因为由 IEEE 802.11 所支持的对高层连接的维护不能得到保证，因而服务可能受到

破坏。

2．介质访问存取控制技术

IEEE 802.11 工作组考虑了两种 MAC 算法：一种是分布式访问控制协议，像 CSMA/CD 一样，利用载波监听机制；另一种是中央访问控制协议，由中央决策者进行访问的协调。分布式访问控制协议适用于由地位等同的工作站组成的网络以及具有突发性通信的无线局域网的基站所组成的网络。中央访问控制协议对于那些具有时间敏感数据或者高优先权数据的网络特别有用。

IEEE 802.11 最终形成的一个 MAC 算法称为 DFWMAC（分布式基础无线 MAC），它提供分布式访问控制机制，处于其上的是一个任选的中央访问控制协议，如图 9-4 所示。在 MAC 层中靠下面的是分布协调功能子层（DCF），DCF 利用争用算法为所有的通信提供访问控制。一般异步通信用 DCF。在 MAC 层中靠上面的是点协调功能（PCF），PCF 用中央 MAC 算法，提供无争用服务。PCF 位于 DCF 的上面，并利用 DCF 的特性来保证用户的介质访问。

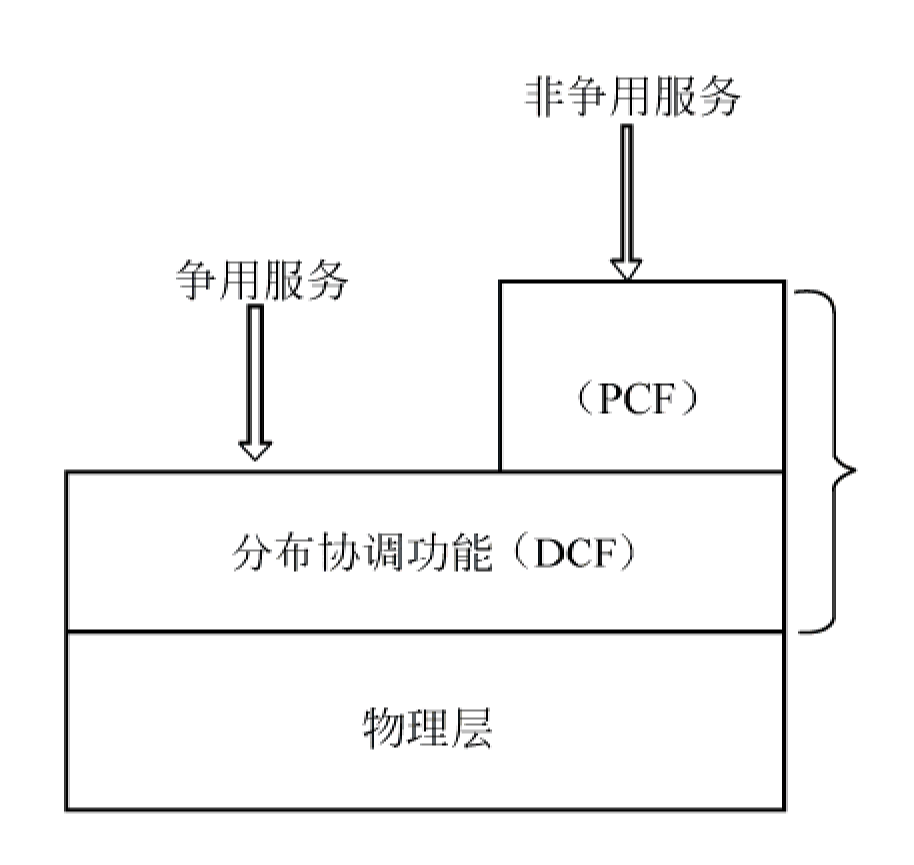


图 9-4　IEEE 802.11 协议结构

DCF 子层介质存取方式采用 CSMA/CA（Carrier Sense Multiple Access with Collision Avoidance）算法。与以太网所采用的 CSMA/CD 很相似，只不过 DCF 没有冲突检测功能，因为在无线网上进行冲突检测是不太现实的。介质上信号的动态范围非常大，因而发送站不能有效地辨别出输入的微弱信号是噪声还是站点自己发送的结果。所以取而代之的方案是采用一种碰撞避免（Collision Avoidance）的算法。具体地说为了保证上述 CSMA 算法的顺利和公平，DCF 采用了一系列的延迟，称为帧间空隙（IFS），相当于一种优先权机制。利用 IFS 延迟的 CSMA/CA 访问控制的操作过程如下：

（1）发送站监听，如介质空闲，站点再继续监听一段时间（一个 IFS 的延迟），如果在这段时间内介质仍然是空闲的，则站点可立即发送。

（2）如果介质忙，站点继续监听介质，直到完成当前的传输。

（3）一旦当前的传输已完成，站点要继续监听一段时间（一个 IFS 的延迟）。如在此

期间介质仍然空闲，然后站点按照二进制指数退避一段时间后监听介质，如果介质仍然空闲，站点就可以发送下一个数据帧。

帧间空隙（IFS）有三种不同的优先权值来提供介质访问控制：

（1）短帧间空隙（SIFS）。最短的 IFS，用于所有的立即相应活动。

（2）点协调功能的帧间空隙（PIFS）。中等长度的 IFS，在 PCF 机制中的中央控制器发出查询时用。

（3）分布协调功能的帧间空隙（DIFS）。最长的 IFS，作为异步帧争用访问控制中最小的延时。

SIFS 具有最高的优先权，因为相对于那些需要等待 PIFS 或 DIFS 的站点来说，这些站点总是能优先获取到介质的访问权。PIFS 由中央控制器用于发送查询帧，使它领先于一般的争用通信。DIFS 用于所有普通的异步通信。

3．WLAN 物理层和服务

WLAN 物理层规定了使用的传输技术，服务规定了 WLAN 所提供的功能。

802.11 使用了 5 种传输技术：

（1）红外：使用 0.85μm 或 0.95μm 波段上的漫射传输，允许 1Mbps 或 2Mbps 的速率，它无法穿过墙壁，带宽低，不是很通用的方案。

（2）FHSS（跳频扩频）：短距离的无线电波，使用了 79 个 1MHz 的信道，抵干扰能力强，主要缺点是带宽低。

（3）DSSS（直接序列扩频）：也是短距离的无线电波，也被限制在 2Mbps 的速率上。

（4）OFDM（正交频分多路复用）：可以达到 54Mbps，频谱效率高，抗干扰性强。

（5）HR-DSSS（高速率的直接序列扩频）：可达到 11Mbps，称为 802.11b。它的覆盖范围可以是 OFDM 的 7 倍。

服务包括 5 种分发服务和 4 种站服务。分发服务涉及到对单元的成员关系的管理，并且会影响单元外的站；而站服务则只与一个单元内部的活动有关系。5 种分发服务是由 AP 提供的，它们处理站的移动性，进入单元时进行关联，离开单元时断开联系：

（1）关联：移动站利用该服务连接到 AP 上。

（2）分离：移动站离开或关闭时解除关联关系。

（3）重新关联：改变其首选 AP。

（4）分发：决定如何路由那些发送给 AP 的帧。

（5）融合：使用非 802.11 的网络发送信息。

而内部单元则包括 4 种站服务：

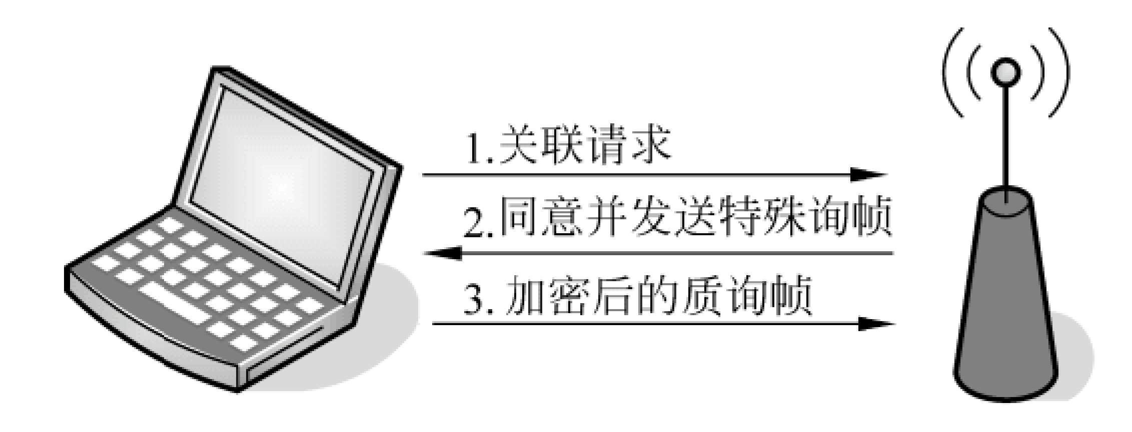
（1）认证：在 WLAN 中，每一个站都必须证明自己的身份才能够发送数据。整个过程如图 9-5 所示。

（2）解除认证：已经通过认证的移动站要离开网络时，就需要解除认证。

（3）私密性：当 WLAN 需要对发送的信息保密时，可以使用该服务，指定的加密

算法是 RC4。

（4）数据投递：即数据的传输功能。



注：如果 AP 收到正确的加密帧就说明其知道预先分配的口令。

图 9-5 移动站认证过程示意图

4．802.11 系列标准

IEEE 802.11 先后提出了以下多个标准，最早的 802.11 标准只能够达到 1～2Mbps 的速度，在制订更高速度的标准时，就产生了 802.11a 和 802.11b 两个分支，后来又推出了 802.11g 的新标准，如表 9-1 所示。

表 9-1 无线局域网标准

标　准	运 行 频 段	主 要 技 术	数 据 速 率
802.11	2.4GHz 的 ISM 频段	扩频通信技术	1Mbps 和 2Mbps
802.11b	2.4GHz 的 ISM 频段	CCK 技术	11Mbps
802.11a	5GHz 的 U-NII 频段	OFDM 调制技术	54Mbps
802.11g	2.4GHz 的 ISM 频段	OFDM 调制技术	54Mbps

注：ISM 是指可用于工业、科学、医疗领域的频段；U-NII 是指用于构建国家信息基础的无限制频段。

IEEE 802.11a、IEEE 802.11b 或 IEEE 802.11g，主要是以物理层的不同作为区分，所以它们的区别直接表现在工作频段以及数据传输率、最大传输距离这些指标上。而工作在媒介层的标准又分 IEEE 802.11h、IEEE 802.11e 及将来的 IEEE 802.11i 几种标准。

（1）802.11h 是 802.11a 的扩展，目的是兼容其他 5GHz 频段的标准，如欧盟使用的 HyperLAN2。

（2）802.11e 是 IEEE 为满足服务质量（QoS）方面的要求而制订的 WLAN 标准。在一些对时间敏感、有严格要求的业务（如话音、视频等）中，QoS 是非常重要的指标。在 802.11MAC 层，802.11e 加入了 QoS 功能，其中的混合协调功能可以单独使用或综合使用以下两种信道接入机制：一种是基于论点式的（Contention Baased），一种是基于投票式的（Polled）。

（3）IEEE 802.11i 规定使用 802.1x 认证和密钥管理方式，在数据加密方面，定义了 TKIP、CCMP（Counter-Mode/CBC-MAC Protocol）和 WRAP 三种加密机制。其中 TKIP 采用 WEP 机制里的 RC4 作为核心加密算法，可以通过在现有的设备上升级固件和驱动

程序的方法达到提高 WLAN 安全的目的。CCMP 机制基于 AES 加密算法和 CCM（Counter-Mode/CBC-MAC）认证方式，使得 WLAN 的安全程度大大提高，是实现 RSN 的强制性要求。由于 AES 对硬件要求比较高，因此 CCMP 无法通过在现有设备的基础上进行升级实现。WRAP 机制基于 AES 加密算法和 OCB（Offset Codebook），是一种可选的加密机制。

9.1.4　IEEE 802.16 系列标准

最近几年来，无线网络技术作为一种用户接入技术已经成为传统的铜线本地环路技术的一种替代技术，并且越来越受到人们的重视。人们对无线网络技术的兴趣主要集中在无线本地环路 WLL（Wireless Local Loop）或者固定无线接入方面。为了给本地无线环路 WLL 提供一个标准，IEEE 802 委员会于 1999 年成立了 802.16 工作组来专门开发宽带无线标准。

IEEE 802.16 负责对无线本地环路的无线接口及其相关功能制定标准，它由三个小工作组组成，每个小工作组分别负责不同的方面：IEEE 802.16.1 负责制定频率为 10G～60G 赫兹的无线接口标准；IEEE 802.16.2 负责制定宽带无线接入系统共存方面的标准；IEEE 802.16.3 负责制定频率范围在 2GHz～10GHz 赫兹之间获得频率使用许可的应用的无线接口标准。我们可以看到，802.16.1 所负责的频率是非常高的，而它的工作也是在这三个组中走在最前沿的。由于其所定位的带宽很特殊，在将来 802.16.1 最有可能会引起工业界的兴趣。

802.16 无线服务的作用就是在用户站点同核心网络之间建立起一个通信路径，这个核心网络可以是公用电话网络也可以是因特网。IEEE 802.16 标准所关心的是用户的收发机同基站收发机之间的无线接口。其中的协议专门对在网络中传输大数据块时的无线传输地址问题做了规定，协议标准是按照三层结构体系组织的。

三层结构中的最底层是物理层，该层的协议主要是关于频率带宽、调制模式、纠错技术以及发射机同接收机之间的同步、数据传输率和时分复用结构等方面的。对于从用户到基站的通信，标准使用的是按需分配多路寻址－时分多址（DAMA-TDMA）技术。按需分配多路寻址（DAMA）技术是一种根据多个站点之间的容量需要的不同而动态地分配信道容量的技术。时分多址（TDMA）是一种时分技术，它将一个信道分成一系列的帧，每个帧都包含很多的小时间单位，称为时隙。时分多路技术可以根据每个站点的需要为其在每个帧中分配一定数量的时隙来组成每个站点的逻辑信道。通过 DAMA-TDMA 技术，每个信道的时隙分配可以动态地改变。

在物理层之上是数据链路层，在该层上 IEEE 802.16 规定的主要是为用户提供服务所需的各种功能。这些功能都包括在介质访问控制（MAC）层中，主要负责将数据组成帧格式来传输和对用户如何接入到共享的无线介质中进行控制。MAC 协议对基站或用户在什么时候采用何种方式来初始化信道做了规定。因为 MAC 层之上的一些层如 ATM

需要提供服务质量服务（QoS），所以 MAC 协议必须能够分配无线信道容量。位于多个 TDMA 帧中的一系列时隙为用户组成一个逻辑上的信道，而 MAC 帧则通过这个逻辑信道来传输。IEEE 802.16.1 规定每个单独信道的数据传输率范围是 2Mbps～155Mbps。

在 MAC 层之上是一个会聚层，该层根据提供服务的不同提供不同的功能。对于 IEEE 802.16.1 来说，能提供的服务包括数字音频/视频广播、数字电话、异步传输模式 ATM、因特网接入、电话网络中无线中继和帧中继。

9.1.5 WLAN 的安装与配置

首先，安装无线网络的核心——无线接入点 AP，由于它的作用是将有线网络的信息转化为无线信号，因此它的位置决定了整个无线网络的信号强度和传输速率。

然后，对 AP 进行相关的配置：

（1）输入 AP 的管理员密码 SSID（也被称为 ESSID 或 Network Name），它用来标识不同的无线网络信号。然后根据 AP 的预设 IP 地址和掩码，设置客户端的 IP 地址与掩码，这样打开 AP 后，无线网卡就能够自行找到。就可以测试无线连接是否正常。

（2）使用 AP 的配置界面设置 IP 分配方式，它提供了“静态分配”和“动态分配”两种方式，建议使用动态方式。

最后，配置安装加密功能。由于默认情况 AP 是不加密的，因此连接成功后应该进入 AP 的配置界面（通常是 Web 式界面）进行修改。802.11b 无线网络最常用的加密手段是 WEP。

（1）配置 AP：在 AP 配置界面的安全选项中，打开 WEP 加密功能，然后输入一段十六进制的字符（字符必须为 0～9 及 a～f）作为加密字串，这个字串一定要记牢，遗失后将无法连接 AP），保存设置后重新启动 AP。而这个加密字串的位数取决于 WEP 类型，如果采用 64 位加密需要输入 10 位的加密字串，如果是 128 位加密则需要输入 26 位的加密字串。

（2）配置客户端：在无线网卡的“属性”项中，将“数据加密（Web 启用）”这一项激活，然后在“网络密钥（encryption）”和“确认网络密钥”两项中填入在 AP 上设置的加密字串。

9.1.6 设置 RADIUS

当无线网络扩大时，安全保护就成为一个重要内容。采用 RADIUS 技术能够给无线网络再增加一层保护，给试图非法进入网络的人增加难度。

RADIUS 主要用于对远程拨入的用户进行授权和认证。它可以仅使用单一的“数据库”对用户进行认证（效验用户名和口令）。在使用 RADIUS 验证时，整个过程为：

（1）客户端发送一个“Access-Request”数据包给 RADIUS 服务器，其中包含了用户名、口令（使用 MD5 加密）、ID 号和用户访问的端口号。如果 RADIUS 服务器在规

定时间内没有访问，则会重发；如果有多个 RADIUS 服务器，则会在多次尝试连接主 RADIUS 服务器失败后，转向使用其他 RADIUS 服务器。

（2）RADIUS 服务器收到“Access-Request”包后，会在认证数据库中查找用户是否存在，如果存在，则提取此用户的信息列表，其中包括了用户的口令、访问端口和访问权限。并根据该信息进行验证。

如果信息被否认，则返回“Access-Reject”数据包，指示此用户非法，还将根据需要返回错误信息。如果信息被确认，则发送“Access-Challenge”数据包给客户端，并加入状态属性等反馈信息。

注：RADIUS 服务器会直接抛弃没有加“共享密钥”的请求。而对于无法满足的请求，会转给其他 RADIUS 服务器。

（3）客户端收到“Access-Challenge”包后，就会再次提交带新请求 ID 的“Access-Request”数据包，其内容与最初的不同的地方在于：“用户名/口令”信息替换为加密信息，加上了“Access-Challenge”的状态属性。

（4）如果所要求的合法，RADIUS 服务器返回一个“Access-Accept”数据包，其中包括了服务类型（可以是 SLIP、PPP、Login User）及相关信息。例如 PPP 中就包括 IP 地址、子网掩码、MTU 和数据包过滤标示等。

归结而言，一个成功的 RADIUS 登录过程一般包括两次握手的过程。首先，客户端发送一个“Access-Request”数据包（包括用户名、口令和访问端口信息）给服务器，以请求验证，RADIUS 服务器通过查询认证数据库进行鉴别，通过认证后，返回“Access-Challenge”应答包给客户端，询问具体的访问请求，并带上状态属性与相关信息；然后，当客户端收到应答包后，用“Access-Challenge”包中的信息组成新的“Access-Request”包，发送给服务器，服务器应答“Access-Accept”包，完成验证登录过程。图 9-6 显示了这个过程。

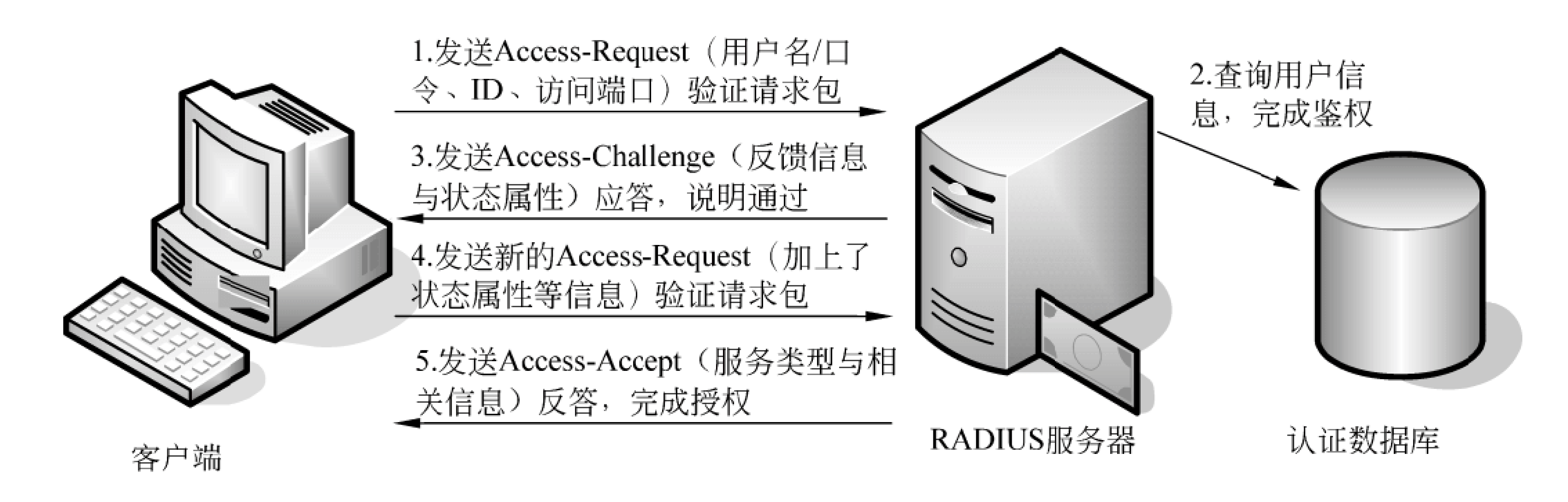


图 9-6　RADIUS 登录过程示意图

9.2 无线通信与 3G 技术

国际电信联盟（ITU）在 2000 年 5 月确定 WCDMA、CDMA 2000 和 TD-SCDMA 三大主流无线接口标准，并将它们写入 3G 技术指导性文件《2000 年国际移动通信计划》（简称 IMT-2000）。

（1）WCDMA。即 Wideband CDMA，意为宽频分码多重存取，其支持者主要是以 GSM 系统为主的欧洲厂商，日本公司也或多或少参与其中。这套系统能够架设在现有的 GSM 网络上，对于系统提供商而言可以较轻易地过渡，而 GSM 系统相当普及的亚洲对这套新技术的接受度预料会相当高。因此 WCDMA 具有先天的市场优势。目前，中国联合网络通信集团公司获得基于 WCDMA 技术制式的 3G 业务经营许可。

（2）CDMA 2000。CDMA 2000 也称为 CDMA Multi-Carrier，以美国高通北美公司为主导提出，摩托罗拉、Lucent 和后来加入的韩国三星都有参与，韩国现在成为该标准的主导者。这套系统是从窄频 CDMA One 数字标准衍生出来的，可以从原有的 CDMA One 结构直接升级到 3G，建设成本低廉。但目前使用 CDMA 的地区只有日、韩和北美，所以 CDMA 2000 的支持者不如 WCDMA 多。目前，中国电信集团公司获得基于 CDMA2000 技术制式的 3G 业务经营许可。

（3）TD-SCDMA。该标准是由中国大陆独自制定的 3G 标准，1999 年 6 月中国原邮电部电信科学技术研究院（大唐电信）向 ITU 提出。该标准将智能天线、同步 CDMA 和软件无线电等当今国际领先技术融于其中，在频谱利用率、对业务支持具有灵活性、频率灵活性及成本等方面的独特优势。另外，由于中国庞大的市场，该标准受到各大主要电信设备厂商的重视，全球一半以上的设备厂商都宣布可以支持 TD-SCDMA 标准。目前，中国移动通信集团公司获得基于 TD-SCDMA 技术制式的 3G 业务经营许可。

下面将 WCDMA、CDMA 2000 和 TD-SCDMA 三种技术进行了归类比较，如表 9-2 所示。

表 9-2　3G 技术比较

比　较	WCDMA	CDMA 2000	TD-SCDMA
核心网	基于 GSM-MAP	基于 ANSI-41	基于 GSM-MAP
双工方式	FDD	FDD	TDD
双向信道带宽（MHz）	10	2.5	1.6
码片速率（Mcps）	3.84	1.2288	1.28
帧长（ms）	10	可变	10（分两个 5ms 子帧）
基站同步	异步（同步可选）	同步	同步
功率控制（Hz）	开环＋快速闭环 1500	开环＋快速闭环 800	开环＋慢速闭环 200

3G 三大技术体制主要的区别是空中接口的不同，即无线传输技术的不同。另外，TD-SCDMA 还采用了智能天线、联合检测、上行同步、接力切换等对系统性能有很大提高的关键技术。

9.3　无线通信与 2.5G 技术

目前已经进行商业应用的 2.5G 移动通信技术是从 2G 迈向 3G 的衔接性技术，由于 3G 是个相当浩大的工程，处于发展的初期，所牵扯的层面多且复杂，要从目前的 2G 迈向 3G 不可能一下子就衔接上，因此出现了介于 2G 和 3G 之间的 2.5G。HSCSD、GPRS、WAP、EDGE、蓝牙（Blue tooth）、EPOC 等技术都是 2.5G 技术。

HSCSD 是 GSM 网络的升级版本，能够将传输速度大幅度提升到平常的 2～3 倍。目前新加坡 M1 与新加坡电讯的移动电话都采用 HSCSD 系统，其传输速度能够达到 57.6Kbps。

GPRS 由于具备立即联机的特性，对于使用者而言，可以说是随时都在上线的状态。GPRS 技术也让服务业者能够依据数据传输量来收费，而不是单纯地以联机时间计费。这项技术与 GSM 网络配合，传输速度可以达到 115Kbps。

EDGE 完全以目前的 GSM 标准为架构，不但能够将 GPRS 的功能发挥到极限，还可以通过目前的无线网络提供宽频多媒体的服务。EDGE 的传输速度可以达到 384Kbps，可以应用在诸如无线多媒体、电子邮件、网络信息娱乐及电视会议上。

WAP 是移动通信与互联网结合的第一阶段性产物，也是大家听说最多的。这项技术让使用者可以用手机之类的无线装置上网，通过小型屏幕遍游在各个网站之间。而这些网站也必须以 WML（无线标记语言）编写，相当于国际互联网上的 HTML（超文件标记语言）。

蓝牙是一种短距的无线通信技术，电子装置彼此可以通过蓝牙连接起来，传统的电线在这里就毫无用武之地了。通过芯片上的无线接收器，配有蓝牙技术的电子产品能够在十米的距离内彼此相通，传输速度可以达到 1Mbps。它避免了以往红外线接口传输技术需要电子线在视线之内的要求。

EPOC 是一种能够让移动电话摇身一变成为无线信息装置（例如智能电话）的操作系统，满足使用者对于数据的需求。它支持信息传送、网页浏览、办公室作业、公用事业以及个人信息管理的应用，也有软件可以和个人计算机与服务器做同步的沟通。

9.4　VoIP 技术

VoIP（Voice over Internet Protocol）是一种以 IP 电话为主，并推出相应的增值业务的技术。它是建立在 IP 技术上的分组化、数字化传输技术，其基本原理是：通过语音压

缩算法对话音进行压缩编码处理，然后把这些语音数据按 IP 等相关协议进行打包，经过 IP 网络把数据报传输到目的地，再把这些语音数据包串起来，经过解码解压处理后，恢复成原来的语音信号，从而达到由 IP 网络传送话音的目的。

VoIP 最大的优势是能广泛地采用 Internet 和全球 IP 互联的环境，提供比传统业务更多、更好的服务。VoIP 可以在 IP 网络上廉价地传送语音、传真、视频和数据等业务，如统一消息、虚拟电话、虚拟语音/传真邮箱、查号业务、Internet 呼叫中心、Internet 呼叫管理、电视会议、电子商务、传真存储转发和其他各种信息的存储转发等。

VoIP 的拓扑结构如图 9-7 所示。

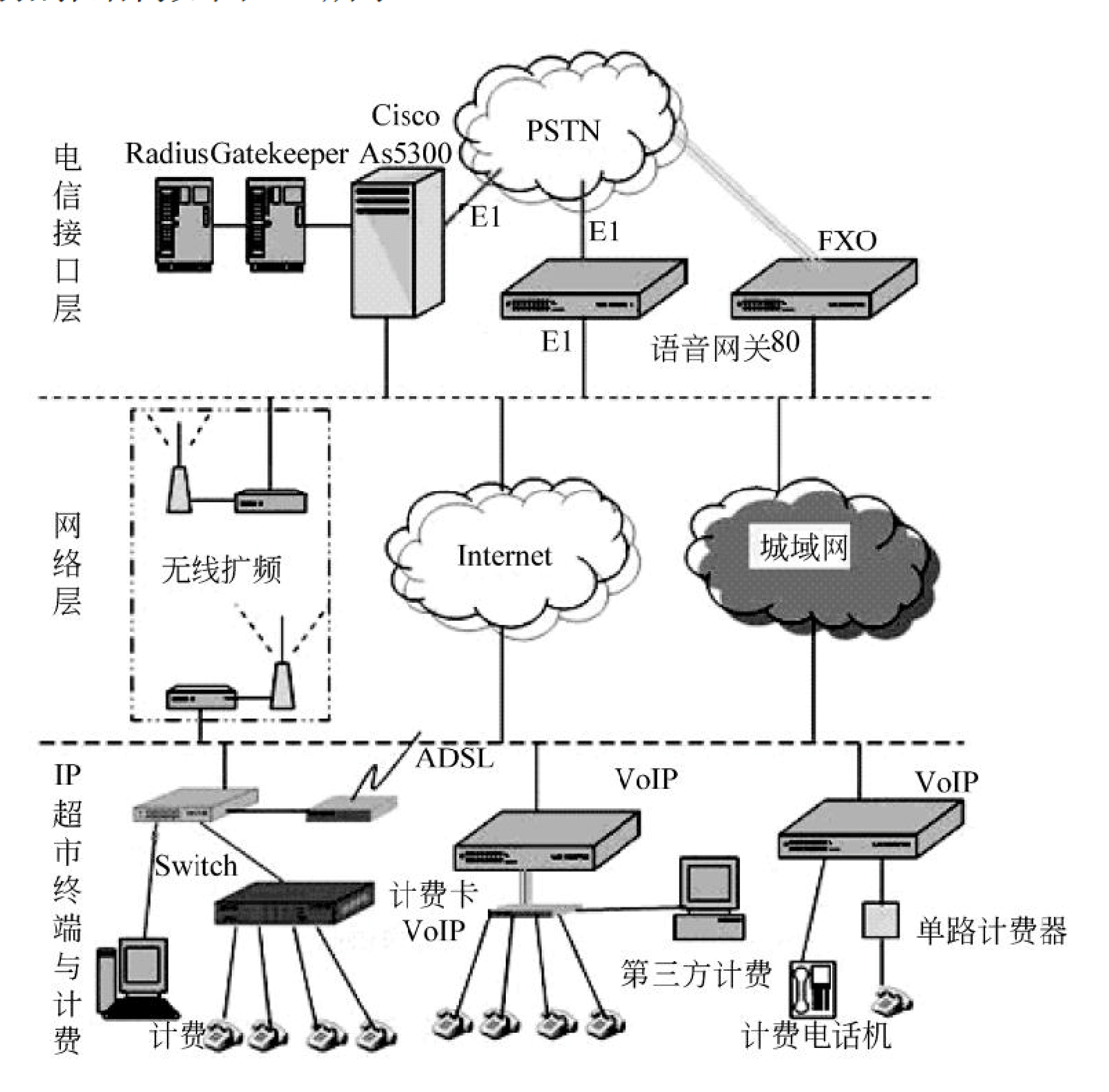


图 9-7 VoIP 的拓扑结构

9.4.1 VoIP 技术的体系结构

VoIP 技术的主要目的是用于处理语音和信令，因此可以将它分为 4 个功能模块：语音包处理模块、电话信令网关模块、网络协议模块、网络管理模块。

（1）语音包处理模块：一般而言，语音包处理模块主要是在数字信号处理器芯片上运行。主要实现以下功能：语音的编码及解码、静音检测、回音抵消器、自适应语音恢复、语音包处理器。

（2）电话信令网关模块：一般而言，电话信令网关模块主要是在 Host CPU 上运行。作为一个“网关处理器”，它主要是作为电话信令，在电讯设备与网络协议处理之间进行协议转换，这些信令包括挂机、摘机、呼入保持、来电显示等。

（3）网络协议模块：这个模块主要是用于处理信令的信息，同时也可以将信令信息转换成对应的特殊网络的信令协议，通过交换网络传输。一般而言，国际上目前比较通用的网络协议标准是 H.323 协议、MGCP 协议和 SIP 协议等。

（4）网络管理模块：主要是提供一个语音管理的接口，实现 VoIP 的配置及维护。管理信息是基于国际标准 ASN.1 及 SNMP（简单网络管理协议）的要求所建立的。

9.4.2　VoIP 的传输过程

VoIP 是以 IP 分组交换网络为传输平台，对模拟的语音信号进行压缩、打包等一系列的特殊处理，使之可以采用无连接的 UDP 协议进行传输。为了在一个 IP 网络上传输语音信号，要求具备几个元素和功能。最简单形式的网络由两个或多个具有 VoIP 功能的设备组成，共同通过一个 IP 网络连接。VoIP 设备先把语音信号转换为 IP 数据流，并把这些数据流转发到 IP 目的地址，IP 目的地址又把它们转换回语音信号。两者之间的网络必须支持 IP 传输，且可以是 IP 路由器和网络链路的任意组合。

VoIP 传输过程可分为语音信号数字化、信号编码分组、信号打包传送、解包及解压缩过程以及数字语音模拟化 5 个过程。

（1）语音信号数字化。语音信号是模拟波形，通过 IP 方式来传输语音。首先要对语音信号进行模拟数据转换，也就是对模拟语音信号进行量化，然后送入到缓冲存储区中。数字化可以使用各种语音编码方案来实现，目前采用的语音编码标准主要有 ITU-TG.711。

（2）信号编码分组。语音信号进行数字编码以后，下一步就要对语音包以特定的帧长进行压缩编码。编码后，压缩的帧合成一个压缩的语音包送入网络处理器。网络处理器为语音添加包头、时标和其他信息后通过 IP 网络传送到另一端。语音网络简单地建立通信端点间的物理连接，并在端点间传输编码信号。IP 网络不会形成连接，而要求把数据放在可变长的数据报或分组中，然后给每个数据报附带寻址和控制信息，并通过网络发送。

（3）信号打包传送。信号（数据）被压缩后，就需要对它进行打包，加进一些协议信息。在收集语音数据的处理过程中需要一些存储时间，因为将语音数据发送到 IP 网络之前必须先收到一定数量的语音数据。在对信号进行编码及压缩过程中，也需要一定的时间来对数据进行存储，从而也产生了一定的时间延迟。

协议信息被加入包中是为了更好地保障完成数据的传输过程。由于 IP 协议是为各种不同的网络互联而设计的，与专用网相比它含有许多复杂的处理过程，它要求将一个包封装到另外一个包中，而且数据在传输的过程中还要经过再打包、重寻址和重新封装等

过程。

（4）解包及解压缩过程。当每个包到达目的地主机（网关、服务器或用户计算机终端）时，要检查该包的序号并将其放到正确的位置，然后用一个解压缩算法来尽量恢复原始信号数据，这时通过利用时钟同步及时延处理技术来填充由发送端处理过程中导致的空缺。由于各个包在传输过程中经过了不同的路由，所以它们到达目的地的顺序有很大差别，因此接收端要将先到达的包放到存储器里一段时间等待后到达的包，等待时间的长短要根据网络的拥塞情况而定。

（5）数字语音模拟化。这个步骤是把前四个步骤所形成的数字语音转换成模拟信号。

在 VoIP 过程中，语音质量下降的根本原因在于，按 Internet 传统纠错机制，接收端如果收到错误的数据报就将其丢弃并请求重传，因此用户最终收到的数据跟原始发送的数据是完全一样的。但是由于 IP 电话业务是一种对时间敏感的业务，不能使用重传机制，这就需要专用的检错和纠错机制来再造声音和填补空隙，需要接收端存储接收到的一定数量的语音数据，然后使用一种复杂的算法来“猜测”丢失包的内容，产生新的语音信息，从而提高通信的质量。因此，接收端听到的语音并不与发送端讲的语音完全一样，其中一部分信息是由 VoIP 系统“再造”的。

9.5 IPv6 协议

希赛教育专家特别提示：本知识点在于掌握 IPv6 协议的主要特点、了解 IPv6 地址的格式以及与 IPv4 地址的兼容性方案，了解 IPv6 相关的一些常识。

IPv6 在 IPv4 的基础上进行改进，它的一个重要的设计目标是与 IPv4 兼容。第一个 IPv6 标准为 IETF 接受并作为 RFC 发布不久，就产生了 6-bone 网络，用于在 IPv6 产品实现广泛商业推广以前，用于测试或获取 IPv6 的经验。它也是中国第一个 IPv6 的商用网。

9.5.1 协议的主要改进

IPv6 对 IPv4 的主要改进如下：

（1）扩展地址：把原来 32 位地址扩展到 128 位，采用 16 进位表示，每四位构成一组，每组间用一个冒号隔开。为了更好地将 IPv4 过渡到 IPv6，IPv6 提供了两类嵌有 IPv4 地址的特殊地址：

0000：0000：0000：0000：0000：FFFF：xxxx：xxxx

或 0000：0000：0000：0000：0000：0000：xxxx：xxxx

其中 xxxx：xxxx 是原来的 IPv4 的 IP 地址。在 IPv6 中有两个特殊了地址：一个是全 0 表示未指定地址；另一个是 0:0:0:0:0:0:0:1 表示环回（Loopback）地址。

（2）简化的包头：IPv6 的包头共有 8 个字段，总长为 40 字节；而 IPv4 的包头则包

含至少 12 个字段，长度在没有选项时为 20 字节，有选项时达 60 字节。IPv6 采用固定格式的包头减少了需要检查和处理的字段的数量，提高选路效率。

（3）对扩展和选项支持的改进：IPv4 可以在 IP 的尾部加入选项，则 IPv6 则将选项加到单独的扩展头中。

（4）流标志：IPv4 对所有的包大致同等对待，这意味着每个包都是由中间路由器按照自己的方式来处理。而路由器并不跟踪任意两台主机间发送的包，因此不能“记住”如何对将来的包进行处理。而 IPv6 中引入了流概念，可以对流中的包进行高效处理。

（5）身份验证和保密：IPv6 使用了两种安全性扩展，分别是 IP 身份验证头和 IP 封装安全性净荷。

9.5.2　IPv6 包头结构说明

如图 9-8 所示，IPv6 协议对其包头定义了 8 个字段。

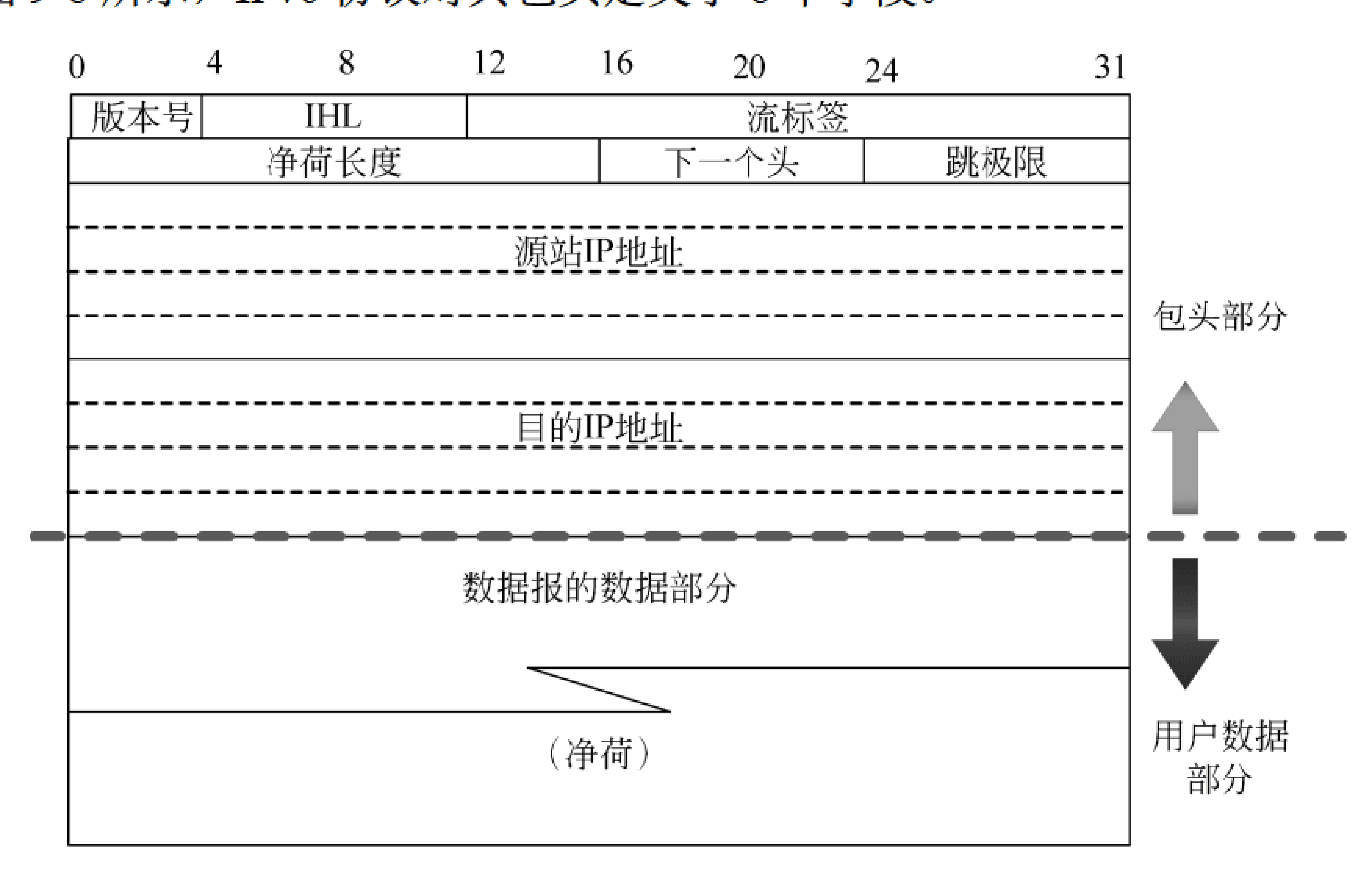


图 9-8　IPv6 包头格式示意图

（1）版本：长度为 6 位，对于 IPv6，本字段的值必须为 6。

（2）类别：长度为 8 位，指明为该包提供了某种“区分服务”。

（3）流标签：长度为 20 位，用于标识属于同一业务流的包（即特定源站到特定目的站），数据流的命名中包括流标签、源节点地址、目的节点地址。

（4）净荷长度：长度为 16 位，包括净荷的字节长度。

（5）下一个头：长度为 8 位，指出了 IPv6 头后所跟的头字段中的协议类型（指出高层是 TCP 来是 UDP）。

（6）跳极限：长度为 8 位，每转发一次该值减 1，到 0 则丢弃，用于高层设置其超

时值。

（7）源地址：长度为 128 位，指出发送方的地址。

（8）目标地址：长度为 128 位，指出接收方的地址（可以是单播、组播或任意点播地址）。

9.5.3　IPv6 的路由原理

在路由和转发过程中，IPv6 路由查找思想与 IPv4 相同，采用最长地址匹配，选择最优路径，同样允许路由过滤、引入、聚合等操作。IPv4 的动态路由协议，经过扩展后可以在 IPv6 网络上运行，包括 RIPng、BGP4＋、ISISv6、OSPFv3。

9.5.4　IPv6 的域名解析

虽然 IPv6 协议将取代 IPv4 的互联网协议，但是有许多部分还是继承了现行 IPv4 的优点的。如域名系统 DNS 就是继续了 IPv4 现行协议。IPv6 网络中的 DNS 同样非常重要，一些 IPv6 的新特性和 DNS 的支持密不可分。

IPv6 网络中的 DNS 与 IPv4 的 DNS 在体系结构上是一致的，都是采用树型结构的域名空间。虽然 IPv4 协议与 IPv6 协议是存在着相当大区别的两套协议，但这并不意味着需要单独两套 DNS 体系，相反在 DNS 的体系和域名空间上两者必须是一致的，IPv4 和 IPv6 共同拥有统一的域名空间。在 IPv4 到 IPv6 的过渡阶段，域名可以同时对应于多个 IPv4 和 IPv6 的地址。随着 IPv6 网络的普及，IPv6 地址将逐渐取代 IPv4 地址。

9.5.5　从 IPv4 到 IPv6 的过渡方案

IPv6 的部署大致要经历一个渐进的过程。初始阶段，在 IPv4 的网络海洋中，会出现若干局部零散的 IPv6 孤岛，为了保持通信，这些孤岛通过跨越 IPv4 的隧道彼此连接。随着 IPv6 大规模的应用，原来的孤岛逐渐聚合成为了骨干的 IPv6 Internet 网络，形成与 IPv4 骨干网并存的局面。在 IPv6 骨干上可以引入了大量的新业务，同时可以充分发挥 IPv6 的优势。

为了实现 IPv6 和 IPv4 网络资源的互访，还需要转换服务器以实现 IPv6 和 IPv4 的互通。

最后，IPv4 骨干网逐步萎缩成局部的孤岛，通过隧道连接，IPv6 占据了主导地位，具备全球范围的连通性。IPv6 提供很多过渡技术来实现这个渐进过程。这些过渡技术主要围绕着解决两类问题：IPv6 孤岛互通技术——实现 IPv6 网络和 IPv6 网络的互通；IPv6 和 IPv4 互通技术——实现两个不同网络之间互相访问资源。

目前有很多种过渡技术方案，其中有两种最基本过渡技术，即双协议栈和隧道。

（1）双协议栈技术。IPv6 和 IPv4 是功能相近的网络层协议，两者都基于相同的物理平台，而且加载于其上的传输层协议 TCP 和 UDP 又没有任何区别。如果一台主机同

时支持 IPv6 和 IPv4 两种协议，那么该主机既能与支持 IPv4 协议的主机通信，又能与支持 IPv6 协议的主机通信，这就是双协议栈技术的工作机理。

（2）隧道技术。随着 IPv6 网络的发展，出现了许多局部的 IPv6 网络，但是这些 IPv6 网络需要通过 IPv4 骨干网络相连。如果将这些孤立的“IPv6 岛”相互连通必须使用隧道技术。利用隧道技术可以通过现有的运行 IPv4 协议的 Internet 骨干网络（即隧道）将局部的 IPv6 网络连接起来，因而是 IPv4 向 IPv6 过渡的初期最易于采用的技术。路由器将 IPv6 的数据分组封装入 IPv4，IPv4 分组的源地址和目的地址分别是隧道入口和出口的 IPv4 地址。在隧道的出口处，再将 IPv6 分组取出转发给目的站点。隧道技术只要求在隧道的入口和出口处进行修改，对其他部分没有要求，因而非常容易实现。但是隧道技术不能实现 IPv4 主机与 IPv6 主机的直接通信。

9.6　例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 8 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

将 IEEE 802.11 与 IEEE 802.3 相比较，得出的正确结论是<u>（1）</u>。

（1）A．DCF 子层与 MAC 子层功能完全相同

B．DCF 子层没有冲突检测功能

C．DCF 子层与 MAC 子层功能完全不相同

D．DCF 子层也需要有冲突检测

例题 1 分析

DCF 子层介质存取方式采用 CSMA/CA 算法，假如站点要发送 MAC 帧，它先监听介质，如果介质是空闲的，则发送一帧，否则站点必须等待，直到正在进行的传输完成后才能发送。它与以太网所采用的 CSMA/CD 很相似，只不过 DCF 没有冲突检测功能，无线介质上信号的动态范围非常大，因而发送站不能有效地辨别出输入的微弱信号是噪声还是站点自己发送的信号，所以答案选 B。

例题 1 答案

（1）B

例题 2

下面关于 IPv6 协议优点的描述中，准确的是<u>（2）</u>。

（2）A．IPv6 协议允许全局 IP 地址出现重复

B．IPv6 协议解决了 IP 地址短缺的问题

C．IPv6 协议支持通过卫星链路的 Internet 连接

D．IPv6 协议支持光纤通信

例题 2 分析

IPv6 地址只是 IPv4 地址的扩展，主要用于解决 IPv4 地址不够用的情况。与 IPv4 地址一样，也是用于 Internet 中表示某个设备的唯一的标识。所以它不允许出现 IP 地址重复的情况。对于 C 和 D 选项，这种说法当然是没错的，但是题目要求的是最准确的选项，故选择 B。

例题 2 答案

（2）B

例题 3

IEEE 802.11 定义了无线局域网的两种工作模式，其中__（3）__模式是一种点对点连接的网络，不需要无线接入点和有线网络的支持。

（3）A．Roaming　B．Ad hoc　C．Infrastructure　D．DiffuseIR

例题 3 分析

本题考查无线局域网的相关概念，无线局域网（WLAN）分为两大流派：一是面向数据通信的计算机局域网发展而来的，采用的是无连接协议，即 IEEE 802.11 标准；另一个是致力于面向语音的蜂窝电话，采用的是基于连接的协议，即 HIPERLAN-2 标准。在“网络管理员”考试中，主要要求掌握的是 IEEE 802.11 标准。IEEE 802.11 标准定义了两种无线网络的拓扑结构：一是基础设施网络（Infrastructure），它是通过无线接入点（AP）将其连到现有网络中；二是特殊网络（Ad hoc），它是一种点对点连接。它不需要无线接入点和有线网络的支持。

例题 3 答案

（3）B

例题 4

IEEE 802.11 MAC 层采用__（4）__协议。

（4）A．CSMA/CA　B．CSMA/CB　C．CSMA/CD　D．CSMA/CF

例题 4 分析

802.11 在 MAC 层采用 CSMA/CA 算法。在无线网上进行冲突检测是不太现实的。介质上信号的动态范围非常大，因而发送站不能有效地辨别出输入的微弱信号是噪声还是站点自己发送的结果。所以取而代之的方案是采用一种碰撞避免（Collision Avoidance）算法。

例题 4 答案

（4）A

例题 5

下面的无线通信技术中，通信距离最短的是__（5）__。

（5）A．蓝牙　B．窄带微波　C．CDMA　D．蜂窝通信

例题 5 分析

所谓蓝牙（Bluetooth）技术，实际上是一种短距离无线通信技术，利用“蓝牙”技术，能够有效地简化掌上电脑、笔记本计算机和移动电话等移动通信终端设备之间的通信，也能够成功地简化以上这些设备与 Internet 之间的通信，从而使这些现代通信设备与因特网之间的数据传输变得更加迅速高效，为无线通信拓宽道路。说得通俗一点，就是蓝牙技术使得现代一些轻易携带的移动通信设备和计算机设备，不必借助电缆就能联网，并且能够实现无线上因特网，其实际应用范围还可以拓展到各种家电产品、消费电子产品和汽车等信息家电，组成一个巨大的无线通信网络。

蓝牙是一种低成本、大容量的短距离无线通信规范。蓝牙比红外的优越性在于，它的传输距离远（10～100 米不等）、传输速度快。

蜂窝移动通信是采用蜂窝无线组网方式，在终端和网络设备之间通过无线通道连接起来，进而实现用户在活动中可相互通信。其主要特征是终端的移动性，并具有越区切换和跨本地网自动漫游功能。蜂窝移动通信业务是指经过由基站子系统和移动交换子系统等设备组成蜂窝移动通信网提供的话音、数据、视频图像等业务。

微波通信是长途、大容量通信的无线传输手段。是利用微波信道传输数字信号，因为基带信号为数字信号，所以称为数字微波通信系统。按微波通信的性能可概括为：① 微波，指通信频率是微波频段（分米波、厘米波、毫米波）。它不受天气和工业干扰及太阳黑子变化的影响，可靠性高，天线尺寸小。② 多路，指微波通信设备的能频带可以做得很宽，传输容量大，可传输的话路数是相当多的。

例题 5 答案

（5）A

例题 6

无线城域网标准 IEEE 802.16 规定的有效覆盖范围最大可达__（6）__。

（6）A．2km　　B．5km　　C．10km　　D．30km

例题 6 分析

IEEE 802.16 又称为 IEEE Wireless MAN 空中接口标准，是适用于 2～66 GHz 的空中接口规范。由于它所规定的无线接入系统覆盖范围可达 30km，因此 802.16 系统主要应用于城域网，被视为可与 DSL 竞争的“最后一公里”宽带接入解决方案。根据使用频段高低的不同，802.16 系统可分为应用于视距和非视距两种，其中使用 2～11GHz 频段的系统应用于非视距范围，而使用 10～66GHz 频段的系统应用于视距范围。根据是否支持移动特性，IEEE 802.16 标准系列又可分为固定宽带无线接入空中接口标准和移动宽带无线接入空中接口标准，其中的 802.16、802.16a、802.16d 属于固定无线接入空中接口标准，而 802.16e 属于移动宽带无线接入空中接口标准。

例题 6 答案

（6）D

例题 7

关于 IPv6，下面的论述中正确的是__（7）__。

（7）A．IPv6 数据包的首部比 IPv4 复杂

B．IPv6 的地址分为单播、广播和任意播三种

C．主机拥有的 IPv6 地址是唯一的

D．IPv6 地址长度为 128 比特

例题 7 分析

IPv6 是 TCP/IP 协议族中的核心协议之一——IP 协议的升级版，它把原来 32 位地址扩展到 128 位，采用 16 进位表示，每四位构成一组，每组间用一个冒号隔开。而且采用了更简化的包头，减少了需要检查和处理的字段的数量，提高选路效率。对于任意一台主机，都可以安装多块网卡，每块网卡都可以赋予多个 IP 地址。

例题 7 答案

（7）D

例题 8

CDMA 系统中使用的多路复用技术是__（8）__。

（8）A．时分多路　　B．波分多路　　C．码分多址　　D．空分多址

例题 8 分析

CDM 是靠不同的编码来区分各路原始信号的一种复用方式，主要和各种多址技术（诸如码分多址 CDMA、频分多址 FDMA、时分多址 TDMA、同步码分多址 SCDMA）结合产生了各种接入技术，包括无线和有线接入。

例题 8 答案

（8）C

第 10 章　小型局域网的组建

局域网是一种用于小范围，短距离内计算机之间进行数据通信和资源共享的小型网络系统。局域网技术目前发展非常迅速，是计算机领域研究和应用的热点。

根据考试大纲的要求，网络管理员考试要求掌握小型网络系统的设计、构建、安装和调试，中小型局域网的运行维护和日常管理等知识。

10.1　网络规划设计

网络规划设计是一项非常有挑战性的任务，它不仅仅是要把多台计算机连接在一起，还应具有多种特性以便于升级和管理。要设计出运行可靠、便于升级的网络，设计者必须认识到网络的每一组成部分都可能具有不同设计需求。只包含少量路由节点的网络都有可能产生一些复杂的问题而造成不可预料的后果，而在设计和构建包含成千上万个节点的网络时，遇到的问题就会更多。

10.1.1　网络设计的原则

在网络设计方面，应着重考虑以下几个要素，它们也是网络设计和网络建设的基本原则。

（1）采用先进、成熟的技术。在规划网络、选择网络技术和网络设备时，应重点考虑当今主流的网络技术和网络设备。只有这样，才能保证建成的网络有良好的性能，从而有效地保护建网投资，保证网络设备之间、网络设备和计算机之间的互联，以及网络的尽快使用、可靠运行。

（2）遵循国际标准，坚持开放性原则。网络的建设应遵循国际标准，采用大多数厂家支持的标准协议及标准接口，从而为异种机、异种操作系统的互联提供极大的便利和可能。

（3）网络的可管理性。具有良好的可管理性的网络，网管人员可借助先进的网管软件，方便地完成设备配置、状态监视、信息统计、流量分析、故障报警、诊断和排除等任务。

（4）系统的安全性。一般的网络包括内部的业务网和外部网。对于内部用户，可分别授予不同的访问权限，同时对不同的部门（或工作组）进行不同的访问及连通设置。对于外部的互联网络，要考虑网络“黑客”和其他不法分子的破坏，防止网络病毒的传播。有些网络系统，如金融系统对安全性和保密性有着更加严格的要求。网络系统的安

全性包括两个方面的内容，一方面是外部网络与本单位网络之间互联的安全性问题；另一方面是本单位网络系统管理的安全性问题。

（5）灵活性和扩充性。网络的灵活性体现在连接方便，设置和管理简单、灵活，使用和维护方便等方面。网络的可扩充性表现在数量的增加、质量的提高和新功能的扩充等方面。网络的主干设备应采用功能强、扩充性好的设备，如模块化结构、软件可升级、信息传输速度高、吞吐量大。可灵活选择快速以太网、千兆以太网、FDDI、ATM 网络模块进行配置，关键元件应具有冗余备份的功能。

（6）系统的稳定性和可靠性。选择网络产品和服务器时，最重要的一点应考虑它们的稳定性和可靠性，这也是我们强调选择技术先进、成熟的产品的重要原因之一。关键网络设备和重要服务器的选择应考虑是否具有良好的电源备份系统、链路备份系统，是否具有中心处理模块的备份，系统是否具有快速、良好的自愈能力等。不应追求那些功能大而全但不可靠或不稳定的产品，也不要选择那些不成熟和没有形成规范的产品。

（7）经济性。网络的规划不但要保质保量按时完成，而且要减少失误、杜绝浪费。

（8）实用性。网络设计一定要充分保护网络系统现有资源，同时要根据实际情况，采用新技术和新装备，还需要考虑组网过程要与平台建设及开发同步进行，建立一个实用的网络。力求使网络既满足目前需要，又能适应未来发展，同时达到较好的性能/价格比。

10.1.2 网络建设的标准

网络设计工作必须满足一些标准，只有按一定的标准进行工作，才有交流协作的基础，设计出的系统才更容易实施和维护。因此制定和选择一些网络设计标准对网络设计相当重要。

1）布线标准

在设计时选择一个布线标准对网络实施、检验和维护相当重要。只有几个人同时使用同一种布线标准进行布线，才能保证系统在工作连接处能够正确连接，才能保证在以后的维护和测试工作中容易发现问题和解决问题。

通常布线需要满足 EIA/TIA 568A 标准，或 EIA/TIA 568B 标准，我们必须在其中选择一个进行，它们对线路的组合是不一样的。选择了布线标准后，布线设备（配线架）的选择就需要符合相应的要求，如果使用 EIA/TIA 568A 标准就不要使用 EIA/TIA 568B 标准的设备，并且在制作接头时，也得按 EIA/TIA 568A 标准来做，如不这样做容易造成布线的混乱。

2）节点编码标准

在网络设计时，节点进行统一的编码对实施和以后的维护来讲非常重要，编码后，我们能很容易地从大量的电缆中进行辨认，为此我们应该设计一个容易操作的编码标准。

一般来讲应该将中间节点按层次关系设定，如 MDF、MDF-1、IDF-1-1 等，终端节

点的节点号通常标明楼层号和房间号如 T-101-5A、T-101-6B。

3）设备选择标准

在一个网络中，各种设备必须互相配合，互相兼容，且性能应该一致，质量一致，才会达到最佳效果。为此我们要为设备的选择制定一个标准，我们要对质量、性能、兼容性等制定一个选择基准。选择设备要基于这个标准，设备不能比标准低也不能太高，如果太低就不能承担起其任务，如果太高则会造成浪费。

4）物理安全标准

在网络设计时，网络设备的物理安全也应该有充分的考虑，重要设备应该有足够的安全防护措施。为此我们应该制定各种设备的防火、防潮和接地标准，UPS 标准（注意何种设备应该使用 UPS），重要设备还需要进行上锁的标准。

10.1.3　网络系统的设计

明确了网络系统设计原则、网络建设的标准后，就可以进行实际的网络设计工作了。

1．确定协议

首先，我们要确定应该选用哪种或哪些网络协议才能满足系统的需求，因为网络协议会影响网络的拓扑结构、网络的带宽，甚至传输的距离。

1）数据链路层协议

数据链路层协议的确定对网络相当重要，它完全决定了网络的类型，如使用 IEEE 802.3u 的网络就一定是 100 兆以太网，使用 IEEE 802.5 的网络就是令牌网。我们应该用以太网、令牌网、FDDI、ATM，还是几种协议混用？要解决这个问题，我们要从下面几方面来考虑。

- 原有的网络设备的利用：设计一个系统，我们不得不考虑对原有系统的利用，以降低成本，缩短系统实施周期。这里我们就要考虑，原有的网络设备能否在新的网络协议下运行的问题。
- 网络带宽：如果网络的通信量很低，我们选择 FDDI 和 ATM 这种高带宽、高成本的网络是没有必要的。如果网络的通信量很高，经常要承载多媒体信息的传输，那我们就不能用低速度的网络，如 X.25、IDSN 等。
- 传输距离：各种网络协议传输的距离要求是不同的，有些协议是局域网的协议，如以太网、令牌网，它们只能在很小的范围内建立网络，有些协议却能在很大范围内建立网络，如 FDDI、ATM、X.25、ISDN、DSL、帧中继等。
- 费用问题：选择协议也得考虑费用，每种协议对应的网络设备和服务费用都是不相同的，甚至相差很大，FDDI、ATM、SONET 等设备和服务费用高昂，但速度很快，而 DSL、ISDN 等费用低廉但速度比较慢，我们就需要在速度和费用上进行合理地选择。
- 选择新技术：有些技术和协议被认为是过时的，我们就不应该再选择它，支持它的厂家和设备将会很少，这会给将来的网络扩展和系统维护带来很大的问题。

网络上并不一定只运行单一的网络协议，为了达到网络系统需求常常要将多个网络协议组合起来使用

2）传输层和网络层协议

传输层和网络层协议对网络系统的影响没有数据链路层协议的大，它主要运行在网络终端上，经常是多个协议联合使用。传输层和网络层协议对运行在网络层以上层的设备有一定的影响。如有的路由器只支持 TCP/IP 协议或 IPX/SPX 协议，这样使用此设备，我们就要用相应的协议和它通信，另外有些协议还不支持路由如 NetBEUI，它就不适合在有路由的网络上运行。

2．确定拓扑结构

网络设计的大部分工作应该都是在进行网络拓扑结构的确定上，网络拓扑的设计采用自上而下的方法，先决定整体然后再决定局部。

1）分析原有系统拓扑结构

在设计网络系统时，我们必须考虑对原有系统的利用和继承，如果原有系统的通信线路能在新系统中运行，就没必要进行更换，这样我们就需要将原有的拓扑结构利用起来。如果以前的通信线路没法再使用，我们就需要重新设置通信线路，这样和设计一个全新的系统没有什么两样。

原有系统在新系统中可能只是一个子网络，也有可能新系统是在原系统上进行的节点的扩展，这两种情形下新网络系统的设计可以说是两种概念，后一种情况网络拓扑结构基本没有什么变化，主要考虑设备的添加或更换；而前一种情况需要对网络整体拓扑结构有一个重新设计，设计时还需要考虑对原有系统的连接。

2）确定服务器位置

成功地设计一个网络，其中一个关键在于设计者要了解网络对服务器功能和位置的需求。服务器提供文件共享、打印、通信和应用服务。典型服务器的运行方式不同于工作站，它们运行特定的操作系统，例如 Netware、Windows NT、UNIX 或 Linux。目前每个服务器通常用来提供一种功能，例如 E-mail 或文件共享。

可以把服务器分为两类，企业服务器和工作组服务器。企业服务器支持所有用户在网络上提出的服务请求，如主域控制器、E-mail 服务器、DNS 服务器、Web 服务器等，组织中每个人都需要此类服务。而工作组服务器只为特定的用户群提供如字处理、文件共享等服务，只有部分用户需要这些服务。

企业服务器要放置在主配线设备（Main Distribution Facility，MDF）上，这样服务器的流量只发送到 MDF 而不必通过其他网络进行传输。在理想情况下，工作组服务器要被放置在距离应用其服务的用户群最近的中间配线设备（Intermediate Distribution Facility，IDF）上。现在你的工作只是把服务器直接连接到 MDF 或 IDF 上。把工作组服务器放在离用户最近的线路上，数据流只能通过网络到达 IDF，而这不会影响在这个网络上的其他用户。服务器应该接到交换机或集线器的最大速率的端口上，以给服务器提

供最大的带宽。

3）确定拓扑结构

在一个简单星型拓扑中只有一个布线间，主配线设备中有一个或多个水平交叉连接（Horizontal Cross-connect，HCC）接插面板。HCC 接插面板用来连接水平电缆和局域网交换机端口。局域网交换机的上行端口和其他端口有所不同，它们不是交叉连接的，通过它可以和路由器接插面板的端口相连，路由器再与域网接口或其他网络连接，这样最终端的主机就和路由器端口有了一条完整的物理连接。简单的网络只需要一个布线间就够了。简单局域网如图 10-1 所示。

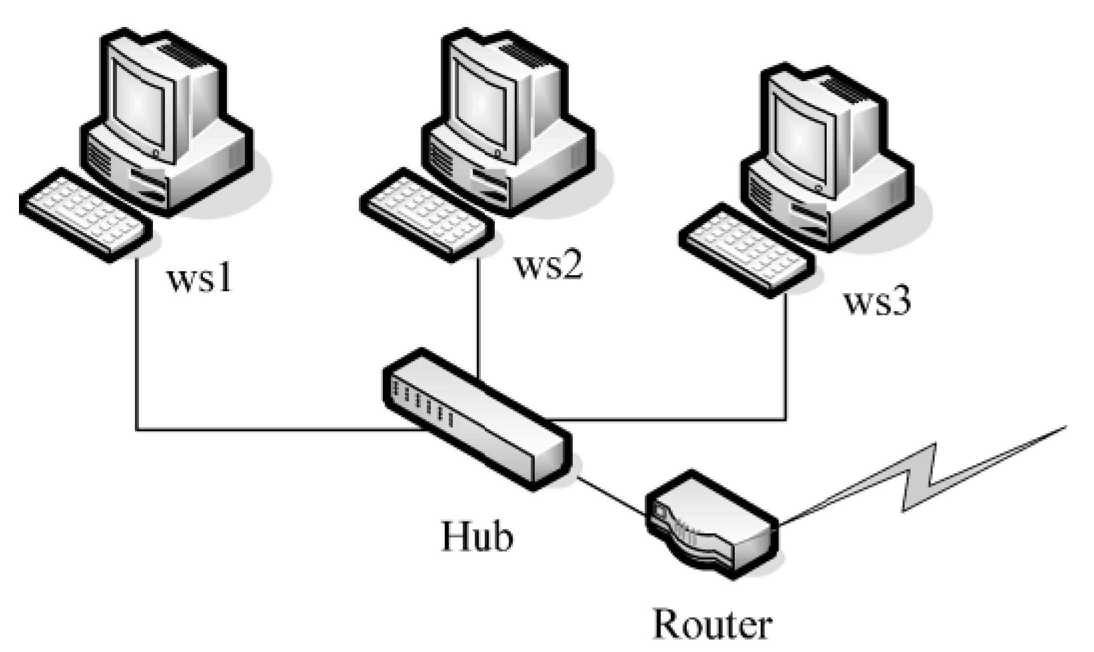


图 10-1　简单局域网

而在一个较大型的网络中，如果主机需要网络进行互连而连接的距离超过了以太网 5 类非屏蔽双绞线连接的 100m 距离限制，通常要设置一个以上的布线间。多个布线间建立以后，就形成了多个汇集区。次一级的布线间被称为中间配线设备 IDF。EIA/TIA 568 标准规定 IDF 应该用垂直电缆（venical cabling），也称为主干电缆（backbone cabling）和主配线设备 MDF 相连。如果垂直电缆的长度超过 100m，就需要将垂直电缆换成多模光纤。这样由 MDF 为中心向外以星型结构逐级辐射，就形成了一个扩展的星形网络。大楼中的局域网如图 10-2 所示。

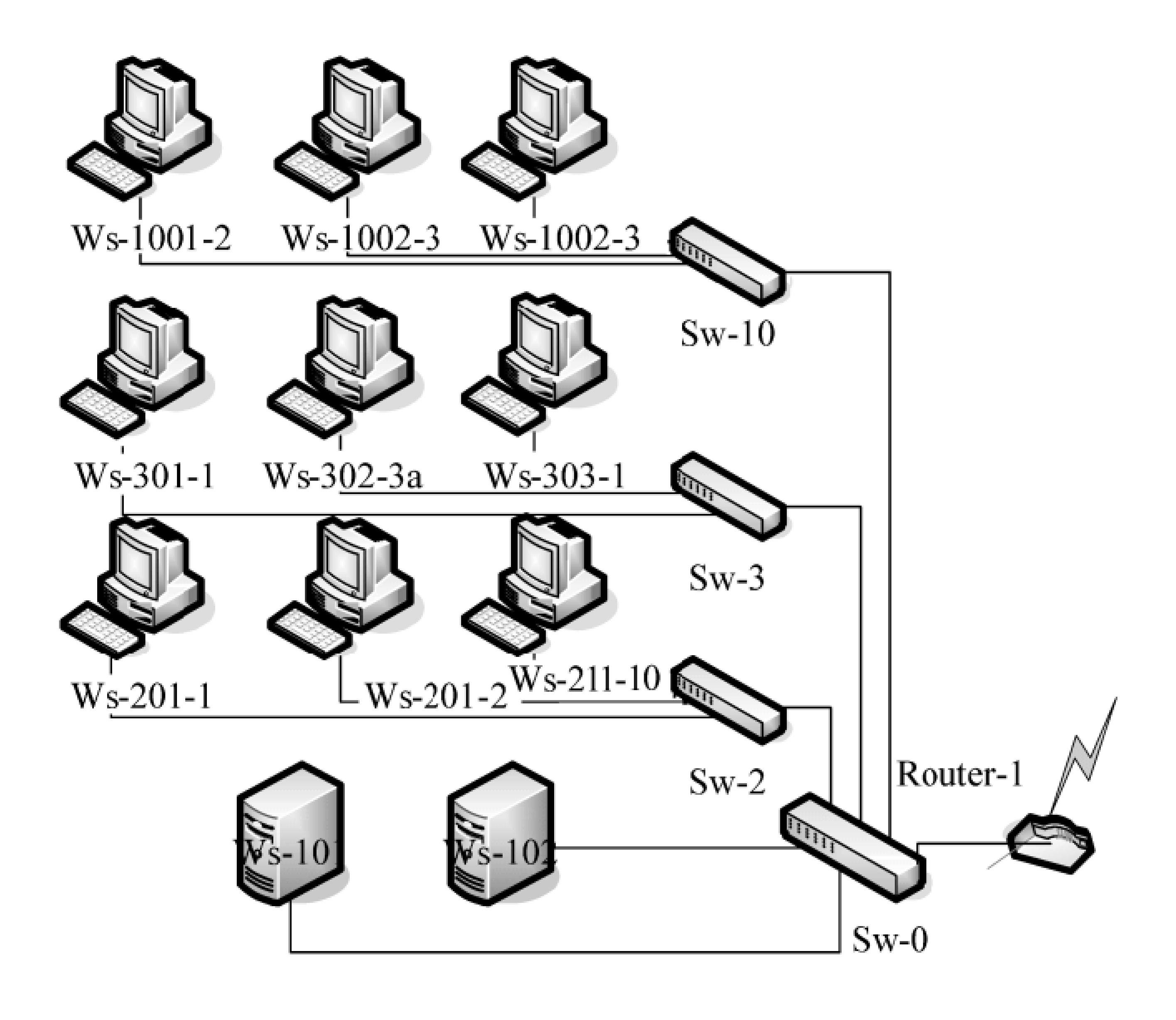


图 10-2　大楼中的局域网

而在更大的网络中，网络的范围扩大到一个校园或一个城市的建筑，建筑和建筑之间的距离达到几公里甚至几十公理的范围，建筑物和建筑物之间就得用 FDDI 或 ATM 网络来进行连接，建筑物内还是采用上面的方式，在每幢大楼中或一个范围内设一个汇接中心，每个汇接中心间使用光纤进行连接。另外因为每个汇接中心下都应该成为一个独立的网络，这时我们应该使用路由器将此网络与其他网络进行隔离。大楼间的局域网如图 10-3 所示。

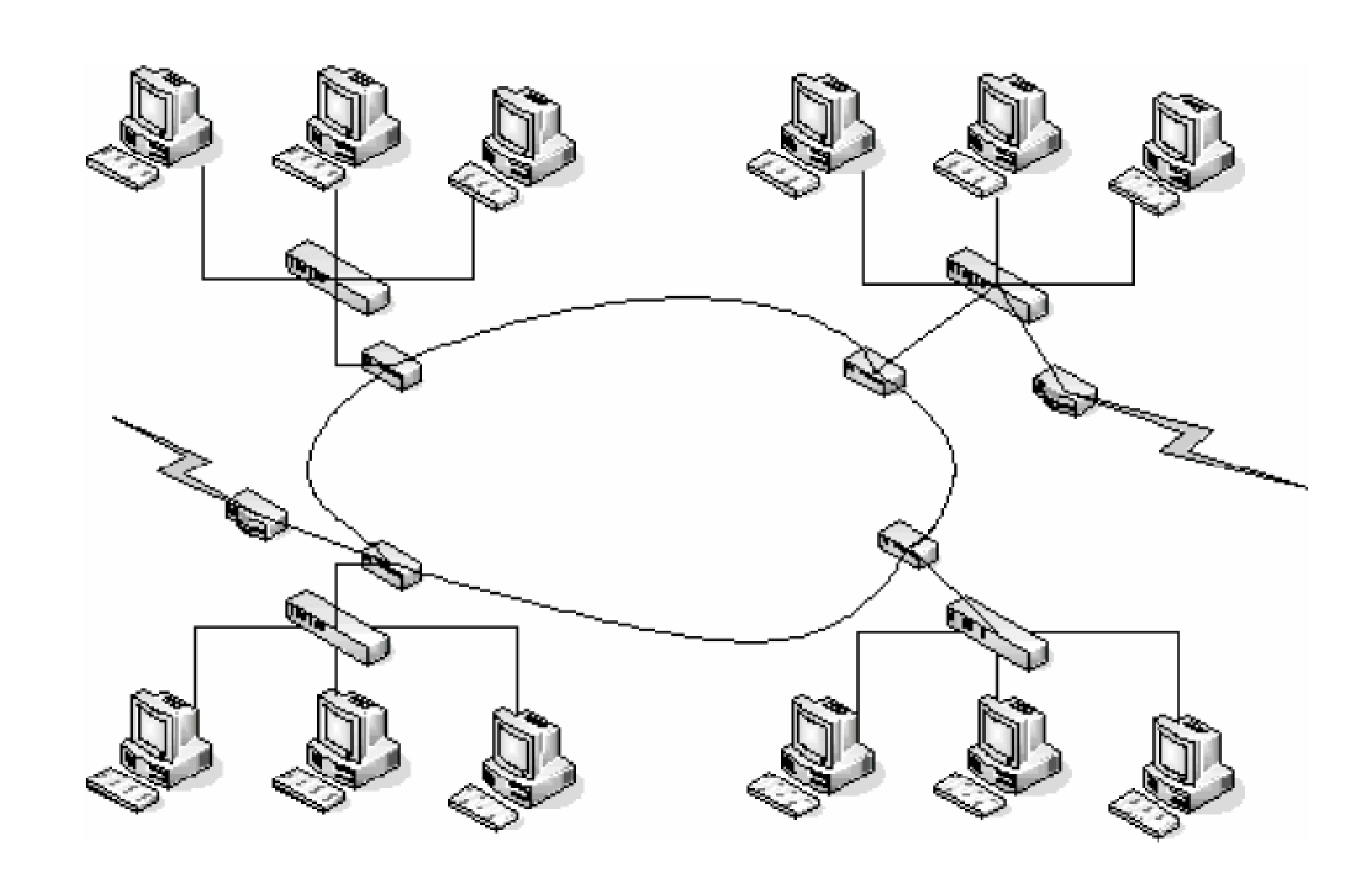


图 10-3 大楼间的局域网

4）确定配线间位置

在一个大楼中，应该在每个楼层都设一个配线间，将 IDF 和一些工作组服务器放置其中，而在大楼的底楼设一个主配线间，将 MDF、企业服务器和路由器等远程联网设备放入其中。当然如果连网的范围不止一幢大楼，那么大楼底只放一个高一级的 IDF，大楼级的 IDF 需要和 MDF 用垂直电缆相连。

在一个楼层中，它应该能保证到达每个终端的距离都不超过 100m 的距离，尽量将其设在楼层的中央，如果即使放在最中央也不能保证到达每个终端的距离在 100m 以内，那就需要在楼层中设置两个或更多的配线间，每个配线间使用垂直电缆和主配线间相连。

配线间应该满足一定的防火、防潮标准，在配线间没有大的电磁干扰，没有高压电线在附近出现，配线间应有很好的接地措施。

配线间还应该满足维护方便的要求，一个大的网络，在物理线路上出故障的几率是相当大的，这就要求我们在设计配线间时，尽可能容易检测出问题所在，并且能方便地将错误排除。

5）节点编号和线路编号

为了更好地标识每个节点和线路，我们在网络拓扑设计时就应该对每个节点和每个线路进行编号。一般来说每个终端节点的编号应该体现出此节点的物理位置，标识出这

个节点的房间号、面板位置号、端口位置号，如 ws-30-3A 就是一个很好的编号。中间节点可以用层次来进行表示，如 MDF0、IDF1、IDF1-1 分别表示 MDF 节点、一级 IDF 节点、二级 IDF 节点。

线路的编号应该与其连接的两个节点的最低级别的节点编号一致，并且在线段的两头都应该进行编号标记，这样以后才好辨认、维护。

3．确定线缆连接

电缆在网络设计中是最重要的组成部分之一，它直接关系到链路的通信能力。设计方案中包括所用布线的类型（典型的铜线电缆或光纤）和整个网络的布线结构，网络传输介质包括第 5 类非屏蔽双绞线（UTP）和光缆及符合 EIA/TIA 568 标准的连接介质。

除了长度限制外，我们还应该仔细考虑各种拓扑结构的优缺点，因为底层的物理线路是网络有效运行的重要保证，在网络运行中出现的大部分问题是物理层的问题。若计划对某网络进行重大改动，应对要升级或重新布线地区的线缆进行彻底的检查。

无论设计新网络还是为已有的网络重新布线，或在原网络上应用新技术，例如高速以太网、ATM 或吉比特以太网技术，至少在布线系统主干上应使用光纤，水平连接线应使用第 5 类非屏蔽双绞线。线路的升级要先于其他应用的升级，而公司必须保证这些系统要符合既定的工业标准，例如 EIA/TIA 568 标准。

EIA/TIA 568 标准规定每台连接到网络的设备要通过电缆连接到一台中心设备，该标准还规定，主机与网络连接的第 5 类非屏蔽双绞线的连接距离不得超过 100m。

双绞线电缆一定要避开高压电缆，如果一定要穿过高压电缆，那只能使用光缆进行连接，只有光缆能够有效地避开电磁干扰。

在安装电缆不方便的地方，或者终端位置不固定的情况应该使用无线网络，使用无线网络时必须了解无线网络的传播范围和容量，使用 IEEE 802.11 的无线 LAN 网络技术，要求传播范围在 300 英尺以内，如果超过这个范围就要考虑其他的无线 MAN 或无线 WAN 技术。

4．确定节点

网络中节点对信号一般进行放大、转发、过滤、路由等处理，节点对信号的处理能力直接关系到网络的通信性能。在进行网络设计时，我们对节点设备的选用特别重要。

由于集线器是每个端口共享带宽的，因此使用集线器时，每个端口的带宽是集线器带宽的十几分之一甚至几十分之一。而交换机给每个端口提供独立的带宽，端口最大的带宽也就是交换机的带宽。交换机完全能代替集线器的功能，能够连上集线器的设备都能够连上交换机而不需要任何接口，使用交换机代替集线器显然能大大地提高网络的通信能力。所以对通信需求比较大的终端应该使其和交换机相连。另外越是接近网络的中心带宽的需求量就越大，所以在核心必须用高速交换机和 IDF 相连，以提高整个网络的通信能力。

路由器可以有效地将数据包从一个网络转移到另一个网络，它根据网络资源的占用情况沿着通信量低、成本最低的路径发送数据包。路由器还要在各网络之间进行隔离，

防止通信繁忙的区域影响到主干网络系统，防止网络速度降低和出现广播风暴。根据路由器的这些特征，应该在通信比较独立的子网之间增加路由器，这可以改善网络的通信能力。

5. 确定网络的性能

网络性能用来衡量网络的可用程度。它受很多因素的影响，包括：吞吐量；响应时间；资源的可利用度。

不同的用户对性能的要求是不同的。例如用户可能要在网络上传输音频信号和视频信号，但是这种服务所需的带宽要远远大于网络主干所能提供的带宽，这样我们就要靠增加更多的资源来提高数据传输的能力，而增加资源就要提高组建网络的费用，网络设计者要寻找能最大限度提高网络速度而费用最少的设计方法。

有些特定的网络应用能产生巨大的流量，因此网络这时有可能产生拥塞，具体情况如：计算机从一个远程节点装载软件；传输大量图像或视频；主数据库的存取；对文件服务器的访问。

我们对这些应用产生的频度和产生的流量进行估计，就可以估算出某段网络需要满足的流量的峰值。然后再与此网段实际设计速率能提供的流量来比较，得出网络能否满足流量需求。

吞吐量实际上和网络传输速率是一致的。计算出网络的设计传输速率，就能基本得到其实际的传输所能提供的吞吐量。传输速率主要由节点的端口提供的速率决定，通过线路两端的设备和其提供的端口速率，我们就能得到此线路的速率了。下面两点是计算线路速率应该要考虑到的：

（1）线路两边接口的速率若不一致，则只能用最小的速率。

（2）交换机端口的带宽就是实际能提供的最大带宽；集线器等共享带宽的设备其上行端口的带宽就是其能够提供的实际最大带宽，各下行端口的带宽是上行端口带宽除以下行端口的总数。

6. 确定可靠性措施

有些网络系统需要很高的可靠性要求，如银行系统、证券系统、电话网络等。在设计网络时我们需要满足用户在网络可靠性方面的要求。为保证网络的可靠性有如下几种手段，在实际设计时应进行综合考虑，合理的选择和组合，这样才能取得最好的设计效果。

1）冗余线路

冗余线路技术就是在网络中设计中，使用两条以上的线缆来连接设备，保证当一条线路出现问题时，可以使用另外的线缆进行通信的方法。例如，由于双绞线比较细，比较容易出现断路的问题，一般的双绞线是由 4 个线对组成的，但目前的标准中只使用了两对线，另两对线备用，如果在使用的两对线中一对或两对出现问题，则可以使用另两对线来替换，而不必费时费力去重新布线。在主干线路上，我们常常需要多布几根线缆，以保证整个系统的可靠性。

2）冗余接口

给设备预留一些冗余接口，通常能保证网络系统的扩展性，也可以给系统一些可靠性保证。一方面发现某些接口损坏后可以用另外的接口来代替，另一方面一些网络设备由于质量或者其他原因，接口长时间满负荷工作的时候，会使性能降低。这时我们对接口进行一些调整（留出一些空接口等）就能解决这些问题。

3）冗余通路

给一些重要的设备如服务器设置两个以上的通路，可以保证这些设备的可靠性，如给服务器设置两个网卡，两个网卡都连接到网络上，这样如果一条线路出现故障，另外一条线路还能继续工作。FDDI 采用双路网络，它本身就有冗余通路。

4）备用设备

给使用频率高的设备设置一个备用设备，可以在此设备出现问题时及时进行更换，这样可以有效地提高系统的维修速度，让系统几乎能不间断地运行。

5）设备保护

UPS 是可以保证系统停电时还能正常运行的设备，同时还能在电压出现异常时保护设备不被损坏，所以对重要的设备都要有 UPS 保护。另外还有一些其他的措施可以从物理上对设备进行保护，如避雷针、保险丝、机架、线路防护等。

6）子网分离

子网分离是使用交换机、路由器等设备分离子网，它可以避免出现问题的子网向其他子网蔓延，如避免出现广播风暴。这样可以保证另外的子网中数据传输的可靠性。

7. 确定安全性措施

网络设计必须考虑安全性方面的需求，在进行设计前，我们必须确定用户网络是否需要连接 Internet；是否有服务器只对部分用户开放；网络是否有不同类型的用户；网络中数据是否是特别机密的数据；数据的转输是否需要进行加密等问题。根据这些问题，我们设计出能满足这些安全需求的网络系统，并且提供给用户一些安全检测和维护的工具。

现在的网络安全技术大致上有两类：一是物理上的安全，二是技术上的安全。

物理安全有两方面的内容：一是保证网络设备的安全，防止非法使用和破坏，它要求我们将服务器、交换机、集线器、路由器等设备集中放在一个能加锁的房间里，并对钥匙进行安全的保管；二是保证线路的安全，如果需要的话应该使用更安全的传输介质，所有的传输介质里，光纤的安全性最高，其次是同轴电缆，再其次是双绞线，最差是无线介质。

技术安全是使用一些技术手段来保证网络系统的安全，它通过密码保护，用户访问权限，访问控制列表，数据加密，数据完整性控制，模糊信息标题等手段来保证网络的安全。常用的安全技术有 VLAN 技术、防火墙技术、密钥交换认证技术等。

在网络系统设计完后，我们还需要对网络安全方面进行评估，检查网络是否能满足系统的需求、网络的安全保障是否全面、是否还存在安全漏洞。

10.2 组网设备的选择

网络设备的选择是否恰当，将影响到构建后的网络系统的工作性能，因此是非常重要的。网络设备的功能选择，不仅要考虑目前阶段的网络需求，还必须有适当的前瞻性，以确保选择的设备应能满足将来一段时间内网络的应用升级。以下将以一个校园网为例介绍，主要的设备选择应该注意以下几个方面：

1．交换机与集线器

对于小规模的网络，例如由十几台计算机组成的校园网，可以选用集线器进行连接，如果计算机的数量达到 20 台以上，应该考虑采用交换机，对于这种小型的网络，在选择交换机或者集线器时，主要考虑的因素是端口数和每个端口的数据传输速率。再就是考虑价格因素，因为即便是指标名称相同，不同品牌间的差价也许很大，通常来说，中国国内产品价格相对较低，而国外公司的同类产品价格要高很多。

如果网络中的计算机数量已经超过 100 台，就该考虑所采用的交换机是否具备堆叠功能了。如果交换机的端口数少于计算机的数量，即便可以通过采用交换机级联的方法增加总的端口数，但级联层数是有限制的，不能超过 4 层。采用具备堆叠功能的交换机，通过堆叠方法增加端口数，就不会存在级联层数的问题，既能增加端口数，又能保证网络具有相当好的性能。

如果网络还要大一些，同时希望获得更好的数据传输延时性，则可考虑在主干网中使用千兆级交换机，而各分支采用百兆级交换机，这样在网中进行多媒体应用就方便得多了，可以建立电子阅览室、视频点播系统等网络应用。

2．路由器与交换机

某些校园网，除了教育功能之外，可能还有其他一些相关的网络应用，例如学校产业，这时网络中的计算机总数极有可能更多。当网络中的计算机超过 250 台时，就必须考虑采用三层交换机，或具有路由功能的交换机了。因为采用局域网技术的校园网通常都使用 C 类 IP 地址，也就是说，任一网段中至多只具有 255 个 IP 地址，而当网络中计算机总数再多时，必须将网络划分成两个或多个网段。为了使不同网段中的计算机能相互通信，必须通过三层交换机的路由功能来实现。尽管也可以采用专门的路由器，但是专业路由器价格较高，地址解析速度也不如三层交换机快，在局域网中使用并不经济。

如果网络应用对于数据的安全性要求比较高，网络可以采用 VLAN 技术，同时也必须配置相应的具有 VLAN 功能的交换机。利用 VLAN 交换机，可以方便地把整个互连的物理网络划分为若干虚拟的子网。各个虚拟子网虽然在物理链路上同属于一个网络，

但各个子网间却不透明，这有助于保证数据的安全。

对于网络管理者来说，如果希望能在网络应用的过程中可以经常获悉网络的数据流量和网络负载情况，以便可以随时优化网络，或为今后的网络升级提供比较可靠的数据分析，那么就应该选择具有网管功能的交换机。通常对网管交换机的管理有以下两种形式。普遍的做法是交换机提供一个串口，网管工作站通过串口线和交换机连接，这种网管的局限是由于串口线长度的限制，使得网管工作站不能离交换机太远。另一种方法是在 TCP/IP 协议的支持下，利用交换机的普通通信端口将网管工作站和交换机连接起来。网管工作站的地理位置可以更灵活一些，而且可管理性也比较强。

3．工作站网卡

网卡作为计算机和交换机或集线器连接的必需设备，选择是否得当，对于工作站的效率是很重要的。通常网卡的选择是根据交换机或者集线器相应端口的速率进行配置的。

4．网络服务器

如果决定了在网络中配备一台专门的计算机，以便能更好地为其他计算机提供数据共享服务，那么最好是在网络中配置一台服务器。同时应该在网络中安装一些专门的网络软件，并分别在服务器端和客户端进行设置。

如果网络规模相对来说比较大一些，而且服务器又需担当诸如 Web 服务、数据库服务等较专业的服务功能，则必须考虑选择一台专业的服务器。因为毕竟服务器的硬件构架更具专业性，适合于提供专门的服务。在网络应用对服务器服务连续性要求很高的情况下，还应该考虑为网络配置一台备份服务器，并在工作时使备份服务器对主服务器进行同步备份。这样即便在主服务器发生故障时，系统也能把服务任务转给备份服务器，保证网络应用的正常进行。当网络应用对数据备份要求很高时，还可以选择具有冗余阵列备份功能的服务器，通过一块 RAID 卡，使数据在多个硬盘之间进行镜像备份，保证当其中一个硬盘发生故障时，可从另一个备份硬盘上进行数据恢复，保障数据的完整性。

10.3　以太网交换机的部署

以太网交换机的部署包括级联（Uplink）模式、堆叠（Stack）模式和混合模式。

1．级联模式

级联是在网络中增加节点数的另一种方法，级联既可使用普通端口也可使用特殊的 UPLink 端口和 MDI 端口。当相互级联的两个端口分别为普通端口和 MDI 端口或 Uplink 端口时，应当使用直通电缆。当相互级联的两个端口均为普通端口或 Uplink 端口或 MDI 端口时，则应当使用交叉电缆。级联可以延长网段长度。

2．堆叠模式

堆叠是通过厂家提供的一条专用连接电缆，从一台交换机的“UP”堆叠端口直接连接到另一台交换机的“DOWN”端口，以实现单台设备端口数的扩充。其作用就像一个模块化交换机一样，堆叠在一起的交换机可以当作一个单元设备来进行管理。由于受到

堆叠线缆长度的限制，两交换机间的距离不会太远。

3．混合模式

在实际应用中，由于网络的复杂性和用户需求的多样性，通常同时使用两种模式进行交换机的部署，即混合模式。

10.4　VLAN 的划分

虚拟局域网（Virtual Local Area Network，VLAN）是指在局域网交换机里采用网络管理软件所构建的可跨越不同网段、不同位置的端到端的逻辑网络。VLAN 是一个在物理网络上根据用途、工作组、应用等来逻辑划分的局域网络，是一个广播域，与用户的物理位置没有关系。

VLAN 中的网络用户是通过 VLAN 交换机来通信的，一个 VLAN 中的成员看不到另一个 VLAN 中的成员。同一个 VLAN 中的所有成员共同拥有一个 VLAN ID，组成一个虚拟局域网络；同一个 VLAN 中的成员均能收到同一个 VLAN 中的其他成员发来的广播包，但收不到其他 VLAN 中成员发来的广播包；不同 VLAN 成员之间不可直接通信，需要通过路由支持才能通信，而同一 VLAN 中的成员通过 VLAN 交换机可以直接通信，不需路由支持。

1．VLAN 划分的功能

（1）提高管理效率：减少网络中站点的移动、增加和改变所带来的工作量，可以大大简化网络配置和调试工作。

（2）控制广播数据：VLAN 内成员共享广播域，VLAN 间的广播被隔离，这样可以提高网络的传输效率，VLAN 利用了交换网络的高速性能。

（3）增强网络的安全性：广播可以将数据传向每一个站点，通过将网络划分为一个个互相独立的 VLAN，对成员进行分组限制广播，并可根据 MAC 地址、应用类型、协议类型等限制成员或计算机对网络资源的访问。

（4）实现虚拟工作组：按应用或功能组建虚拟工作组。

2．VLAN 划分的方法

VLAN 根据不同的需求，可以有多种划分方式，各种方式优缺点比较如表 10-1 所示。

表 10-1　VLAN 划分方式

划　　分	简单描述与优缺点比较	适 用 场 合
基于端口	按 VLAN 交换机上的物理端口和内部的 PVC（永久虚电路）端口来划分 优点：定义 VLAN 成员时非常简单，只要将所有的端口都定义为相应的 VLAN 组 缺点：如果某用户离开原来的端口到一个新的交换机的某个端口，须重新定义	适合于任何大小的网络

续表

划　　分	简单描述与优缺点比较	适 用 场 合
基于 MAC	这种划分 VLAN 的方法是根据每个用户主机的 MAC 地址来划分 优点：当用户物理位置从一个交换机换到其他交换机时，VLAN 不用重新配置 缺点：初始化时，所有的用户都必须进行配置	适用于小型局域网
基于网络协议	VLAN 按网络层协议来划分，可分为 IP、IPX 等 VLAN 网络 优点：用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，并且可以减少网络通信量，可使广播域跨越多个 VLAN 交换机 缺点：效率低下	适用于需要同时运行多协议的网络
基于 IP 组播	IP 组播即认为一个 IP 组播组就是一个 VLAN 优点：更大的灵活性，而且也很容易通过路由器进行扩展 缺点：适合局域网，主要是效率不高	适合于不在同一地理范围的局域网用户组成一个 VLAN
基于策略	基于策略的 VLAN 能实现多种分配，包括端口、MAC 地址、IP、网络层协议等 优点：可根据自己的管理模式和需求来决定选择哪种类型的 VLAN 缺点：建设初期步骤繁复	适用于需求比较复杂的环境
基于用户定义	是指为了适应特别的 VLAN 网络，根据具体的网络用户的特别要求来定义和设计 VLAN，而且可以让非 VLAN 群体用户访问 VLAN，但是需要提供用户密码，在得到 VLAN 管理的认证后才可以加入一个 VLAN	适用于安全性较高的环境

通常将第一种划分方式又叫作静态划分，后面的几种划分方式统称为动态划分。静态划分安全、可靠，易于配置与维护；而动态划分高效、灵活，但安全缺乏保障。

3．VLAN 之间的通信

当 VLAN 交换机从工作站接收到数据后，会对数据的部分内容进行检查，并与一个 VLAN 配置数据库（该数据库含有静态配置的或者动态学习而得到的 MAC 地址等信息）中的内容进行比较后，确定数据去向，如果数据要发往一个 VLAN 设备（VLAN-aware），一个标记（Tag）或者 VLAN 标识就被加到这个数据上，根据 VLAN 标识和目的地址，VLAN 交换机就可以将该数据转发到同一 VLAN 上适当的目的地；如果数据发往非 VLAN 设备（VLAN-unaware），则 VLAN 交换机发送不带 VLAN 标识的数据。

目前，VLAN 之间的通信主要采取如下 4 种方式：

1）MAC 地址静态登记方式

MAC 地址静态登记方式是预先在 VLAN 交换机中设置好一张地址列表，这张表含有工作站的 MAC 地址及 VLAN 交换机的端口号、VLAN ID 等信息，当工作站第一次在网络上发广播包时，交换机就将这张表的内容一一对应起来，并对其他交换机广播。

这种方式的缺点在于，网络管理员要不断修改和维护 MAC 地址静态条目列表，且大量的 MAC 地址静态条目列表的广播信息易导致主干网络拥塞。

2）帧标签方式

帧标签方式采用的是标签技术，即在每个数据包都加上一个标签，用来标明数据包属于哪个 VLAN。这样 VLAN 交换机就能将来自不同 VLAN 的数据流复用到相同的 VLAN 交换机上。这种方式存在一个问题，即每个数据包加上标签，使得网络的负载也相应增加了。

3）虚连接方式

网络用户 A 和 B 第一次通信时，发送地址解析（ARP）广播包，VLAN 交换机将学习到的 MAC 和所连接的 VLAN 交换机的端口号保存到动态条目 MAC 地址列表中，当 A 有数据要传时，VLAN 交换机从其端口收到的数据包中识别出目的 MAC 地址，查动态条目 MAC 地址列表，得到目的站点所在的 VLAN 交换机端口，这样两个端口间就建立起一条虚连接，数据包就可从源端口转发到目的端口。数据包一旦转发完毕，虚连接即被撤销。这种方式使带宽资源得到了很好的利用，提高了 VLAN 交换机效率。

4）路由方式

在按 IP 划分的 VLAN 中，很容易实现路由，即将交换功能和路由功能融合在 VLAN 交换机中。这种方式既达到了作为 VLAN 控制广播风暴的最基本目的，又不需要外接路由器。但这种方式对 VLAN 成员之间的通信速度不是很理想。

10.5 例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 6 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

阅读下列说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】

某一网络地址块 192.168.75.0 中有 5 台主机 A，B，C，D 和 E，它们的 IP 地址及子网掩码如表 10-2 所示。

表 10-2 主机 IP 地址及子网掩码表

主 机	IP 地址	子 网 掩 码
A	192.168.75.18	255.255.255.240
B	192.168.75.146	255.255.255.240
C	192.168.75.158	255.255.255.240
D	192.168.75.161	255.255.255.240
E	192.168.75.173	255.255.255.240

【问题 1】

5 台主机 A，B，C，D，E 分属几个网段？哪些主机位于同一网段？

【问题 2】

主机 D 的网络地址为多少？

【问题 3】

若要加入第六台主机 F，使它能与主机 A 属于同一网段，其 IP 地址范围是多少？

【问题 4】

若在网络中另加入一台主机，其 IP 地址设为 192.168.75.164，它的广播地址是多少？哪些主机能够收到？

【问题 5】

若在该网络地址块中采用 VLAN 技术划分子网，何种设备能实现 VLAN 之间的数据转发？

例题 1 分析

本题是一个子网掩码划分计算的题目。从题目给出的 IP 分配表可以看出，所有的 IP 地址的掩码都是 255.255.255.240。因此使用此掩码划分的子网的 IP 地址段中，每一个段的 IP 地址为 16 个。对于这种复杂子网划分的情况，可以按照表 10-3 所示的步骤来处理。

表 10-3　获取复杂子网划分的网络号

步　　骤	例　　子
写出 IP 地址	192.168.75.18
写出掩码	255.255.255.240
将 IP 转成二进制表示	192.168.75.00010010
将掩码转成二进制表示	255.255.255.11110000
作与操作	11000000 10101000 01001011 00010000
将结果写为十进制	192.168.75.16→网络号

按照步骤，可以先计算出 5 个主机分别属于 3 个网段：192.168.75.16（范围为 192.168.75.16～31）、192.168.75.144（范围为 192.168.75.144～159），192.168.75.160（范围为 192.168.75.160～175）。从掩码和 IP 地址可以知道：A 单独在一个网段，B，C 同一个网段，D，E 同一个网段。

【问题 2】

本题的解答方法与问题 1 的方法是相同的。根据前面所说的方法，我们可以进行相应的计算：

根据表 10-4 获取复杂子网划分的网络号。

表 10-4 获取复杂子网划分的网络号

步　骤	例　子
写出 IP 地址	192.168.75.161
写出掩码	255.255.255.240
将 IP 转成二进制表示	192.168.75.10100001
将掩码转成二进制表示	255.255.255.11110000
作与操作	11000000 10101000 01001011 10100000
将结果写为十进制	192.168.75.16 0→网络号

因此 D 属于 192.168.75.160 网段（范围为 192.168.75.160～175），而该网段的第一个地址 192.168.75.160 为子网地址，而 192.168.75.175 这个地址为子网的广播地址。

【问题 3】

新加入的主机 F，要与 A 处于同一个网段，则必须要在 A 的地址范围，即 192.168.75.16～31 之间，除去 A 本身的地址 192.168.75.18，则可以选用 192.168.75.17，192.168.75.19～30 的任意地址都是可以的。

【问题 4】

新加入的 IP 地址为 192.168.75.164，属于地址段 192.168.75.160～192.168.75.175 段，所以其广播地址是此范围内的最大地址 192.168.75.175。能收到信息的只有同一个网段的才可以，也就是 D 和 E 两个主机。

【问题 5】

VLAN，虚拟局域网，是从一个大的物理网段中逻辑划分的一个子网或由定义的成员组成的一个逻辑的网络段，同一个 VLAN 中的所有设备都是同一广播域（广播域是一组能相互发送广播报文的节点）的成员，划分 VLAN 有很多方法，最基本的一种是基于交换机的端口号划分。VLAN 通过将网络分成小的广播域和子网，可以更加有效地利用带宽；由于 VLAN 间必须进行第 3 层路由选择才能通信，因此可以通过路由器的控制增强安全性；VLAN 允许第 3 层路由选择协议智能地决定到达的目的地的最佳路径，而且还能够进行负载均衡；而且它还可以减少网络故障的影响，以实现对故障组件的隔离。

图 10-4 是一个带了 VLAN 中继连接的 VLAN 实例。在这个实例中将两个交换机不同端口上连接的 PC 组成一个 VLAN。

在同一个 VLAN 中的计算机可以进行通信，而在不同 VLAN 中的计算机则无法直接通信。它们通常处于不同的 IP 网段（或其他网络层协议），同时也处于不同的广播域，需要利用三层交换机或路由器来互连。

例题 1 答案

【问题 1】

3 个子网，A 单独在一个网段；B，C 同一个网段；D，E 同一个网段

【问题 2】

D 的网络地址为 192.168.75.160。

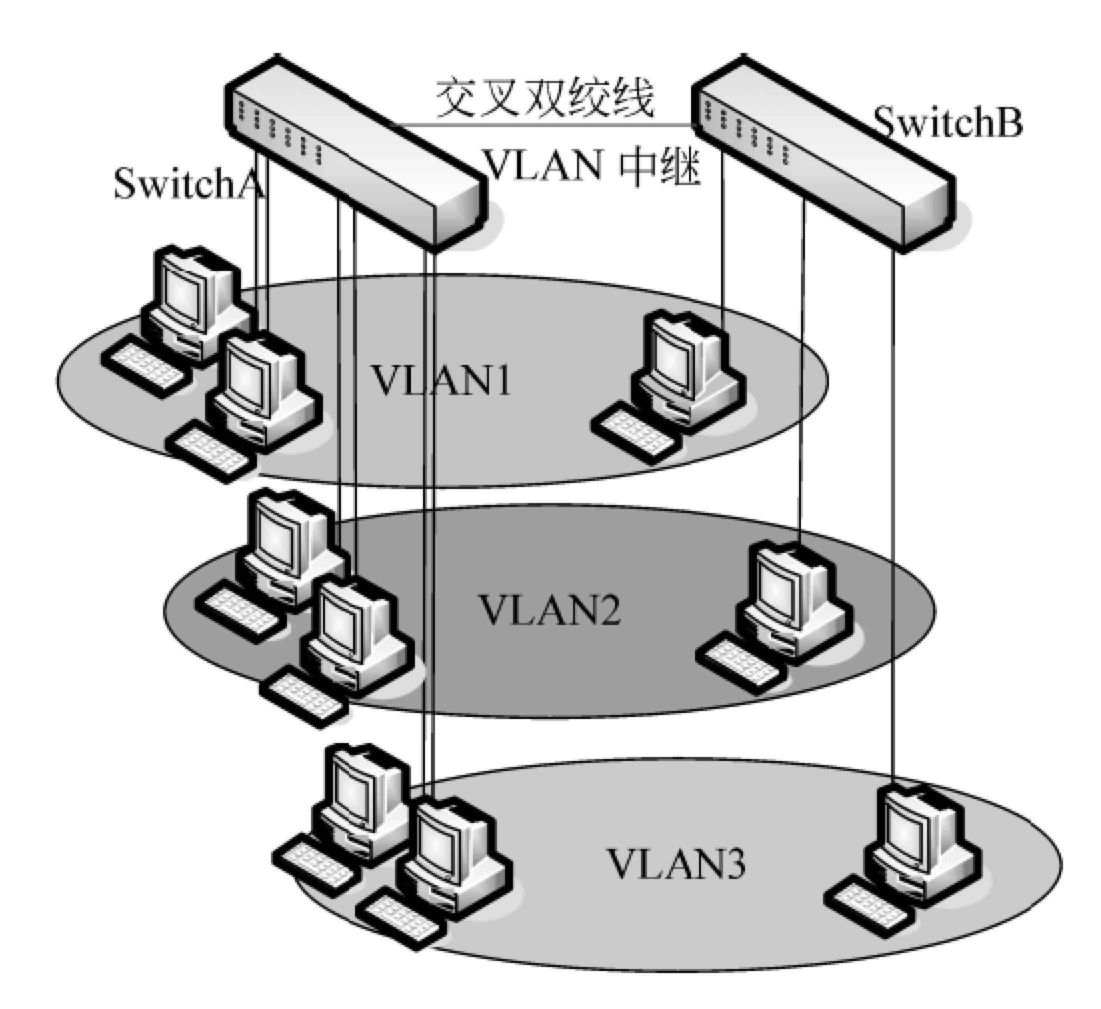


图 10-4　VLAN 实例

【问题 3】

192.168.75.17，192.168.75.19～30

【问题 4】

192.168.75.175

D 和 E 两个主机能收到。

【问题 5】

要使用路由器或三层交换机来实现 VLAN 之间的通信。

例题 2

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某公司 A 楼高 40 层，每层高 3.3 米，同一楼层内任意两个房间最远传输距离不超过 90 米，A 楼和 B 楼之间距离为 500 米，现在需要在整个大楼进行综合布线，结构如图 10-5 所示。为满足公司业务发展的需要，要求为楼内客户机提供数据速率为 100Mbps 的数据、图像，及语音传输服务。

【问题 1】

综合布线系统由六个子系统组成，将图 10-5 中（1）～（6）处空缺子系统的名称填写在答题纸对应的解答栏内。

【问题 2】

考虑性能与价格因素，在图 10-5 中（1）、（2）和（4）中各应采用什么传输介质？

【问题 3】

为满足公司要求，通常选用什么类型的信息插座？

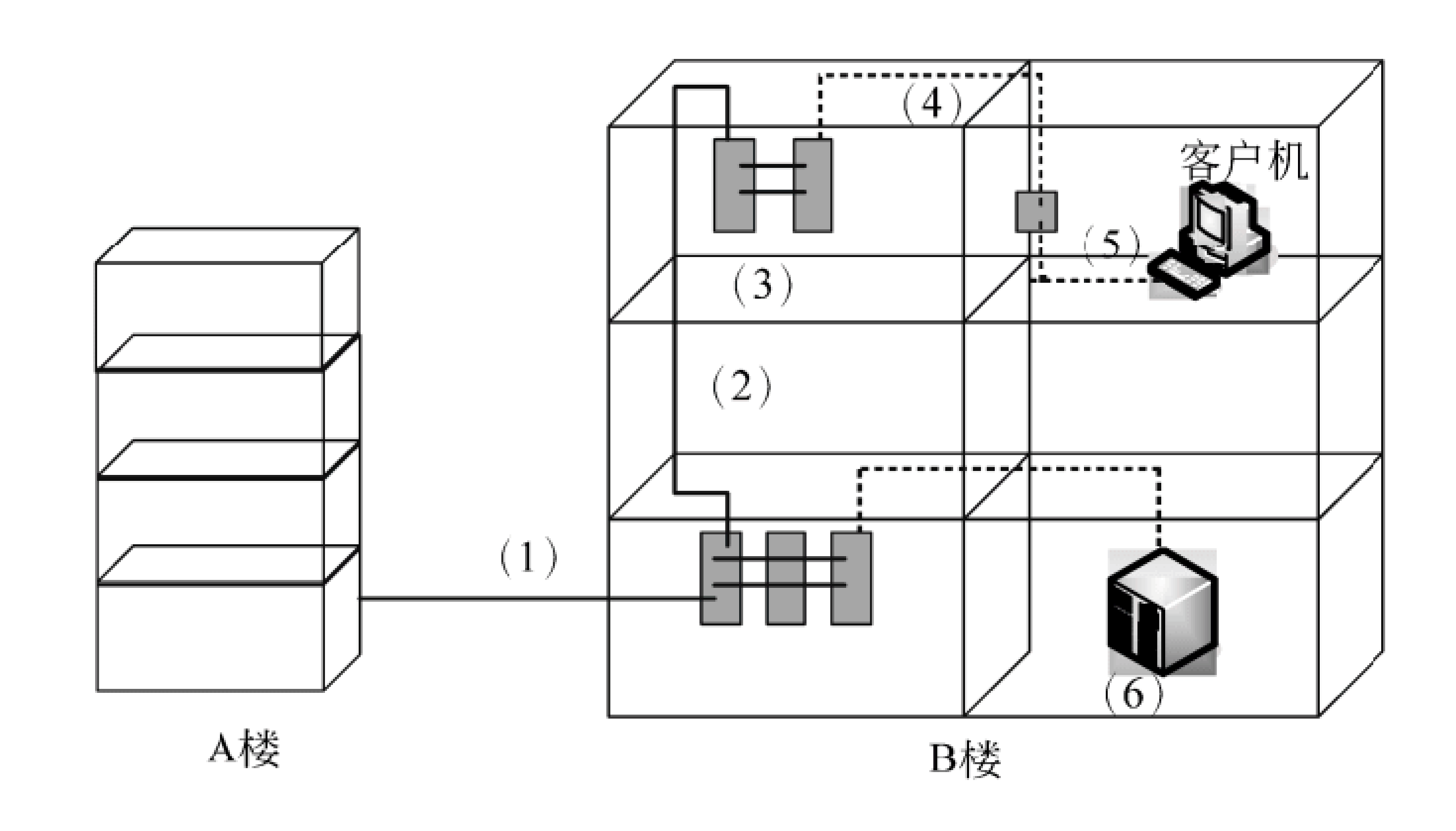


图 10-5　综合布线系统结构示意图

【问题 4】

制作交叉双绞线（一端按照 EIA/TIA 568A 线序，另一端按照 EIA/TIA 568B 线序）时，其中一端的线序如图 10-6（a）所示，将图 10-6（b）中（1）～（8）处空缺的颜色名称填写在答题纸对应的解答栏内。

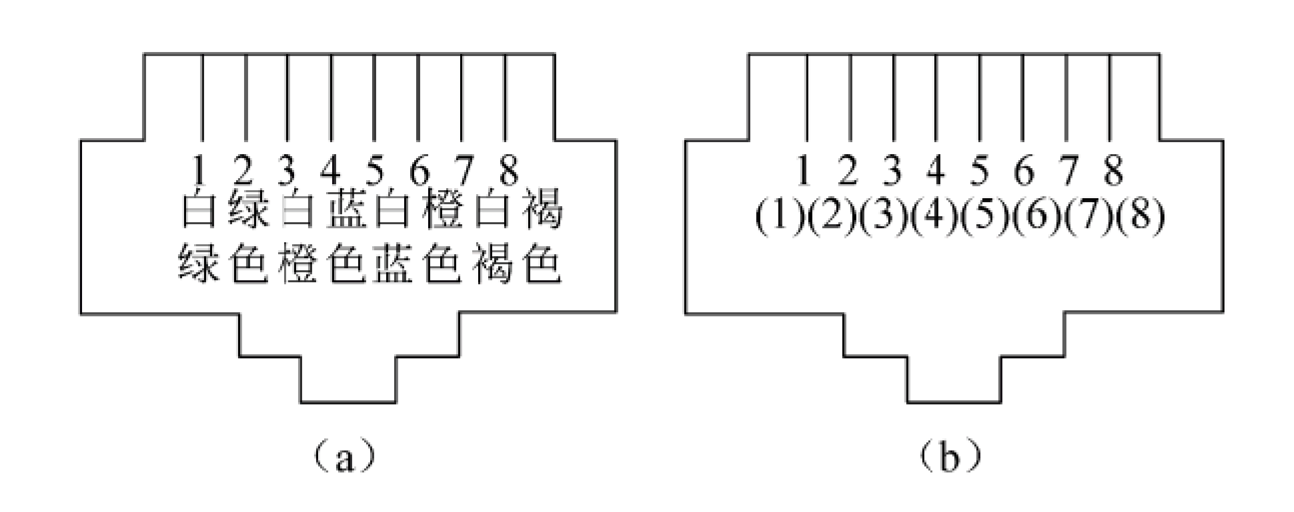


图 10-6　连接器示意图

例题 2 分析

【问题 1】

综合布线系统（Premises Distributed System，PDS）是一种集成化通用传输系统，在楼宇和园区范围内，利用双绞线或光缆来传输信息，可以连接电话、计算机、会议电视和监视电视等设备的结构化信息传输系统。

综合布线系统使用标准的双绞线和光纤，支持高速率的数据传输。这种系统使用物理分层星型拓扑结构，积木式、模块化设计，遵循统一标准，使系统的集中管理成为可能，也使每个信息点的故障、改动或增删不影响其他的信息点，使安装、维护、升级和扩展都非常方便，并节省了费用。

综合布线系统可分为六个独立的系统（模块），如图 10-7 所示。

1）建筑群子系统（户外子系统）

大楼的局域网通常并不是完全封闭的，因此需要与其他大楼的网络相互连接，通常连接的是两个建筑物中的干线子系统，因此在架设时要注意规划管线出入口的位置，以确保能够顺利连接。

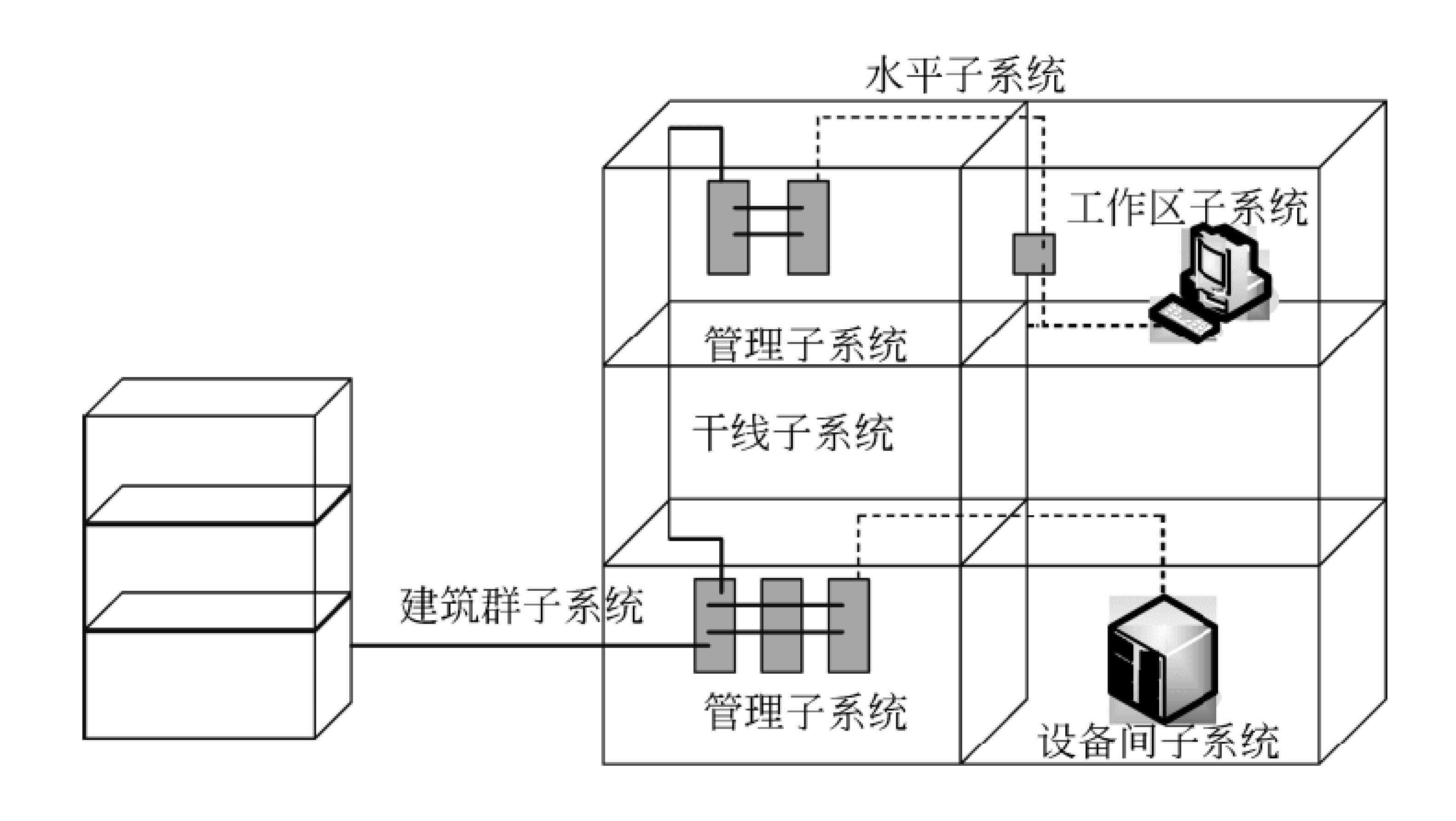


图 10-7　综合布线系统

建筑群子系统包括支持楼群之间通信的传输介质及各种支持设备，如电缆、光缆及电气保护设备。除了各种有线手段之外，建筑群子系统还可以包含其他无线通信手段，如微波、无线电通信等。户外电缆在进入大楼时通常要在入口处进行一次转接，再连入户内系统，而且转接处应该加上防护雷击、外部强电流的电气保护设备。

2）设备间子系统（机房子系统）

基于安全上的考虑，在建筑物的每一个楼层中最好建立一个专门放置网络相关设施的房间，我们将核心网络设备、核心服务器设备、计算机网络通信中枢等设备、UPS 等放在这个房间内。这个子系统并非每一个综合布线系统都有，但在大型建筑物中一般是有的，而且有时还不止一个。

设备间子系统有大量与工作区子系统相似的器件，但由于数量众多，因此所采用的型号与安装方法往往不同，而且设备间子系统通常还集中了大量的通信干线，与户外系统联系密切，因此它通常也包括部分管理子系统的功能。

3）干线子系统

干线子系统将各楼层的管理子系统都串联起来，或者是通过建筑群子系统与其他的建筑物的网络串联起来。因此包括三种电缆：连接各楼层的垂直布线；连接网络机房与大楼主干线的分支电缆；连接不同建筑物的电缆。

由于干线子系统身负连接各个子网络的重任，汇总了各个分支网络的流量，所以在选择主干线的电缆（最适合的线缆有光纤以及无屏蔽的双绞线）和架设方式时，一定要尽可能地提高传输效率。

干线子系统是建筑综合布线系统的骨干，要满足若干小区之间多种通信的需要。从计算机网络的需求来说，它要能够保证所有工作区子系统与机房的连通性，也要保证工作区子系统之间的互通性。

4）管理子系统（布线配线子系统）

在每层楼及机房内都有管理子系统，也称为配线子系统，它们连接着其他各子系统使其构成一个有机的整体，它是实现综合布线系统灵活性的关键。

在现代化综合布线系统中，当发生布线系统需要调整的情况时，可以通过布线配线系统来重新配置布线系统。调整是通过跳线来实现的，跳线有各种类型，有光纤跳线，也有电缆跳线；有单根的，也有多股的。跳线可以很方便地在整个系统中调整各区域内的连接关系，可以将一个工作区子系统方便地连接到另一个设备或是另一个工作区子系统中，这样在搬动设备时只需要将插头取下，到达新的位置后选择合适的插座插上即可，这种方法的优点是显而易见的。

通常管理子系统就像一个大型的橱柜，将所有网络相关的器材整齐地固定在其中，并放置设备中间，以便于管理。

5）水平子系统

以星型拓扑的网络结构而言，水平子系统就是指从管理子系统的配线，加上延伸到使用者身边的信息插座的这段电缆，它包括水平子系统、信息插座、电缆的连接，以及提供跳线用的配线架。

在水平子系统中最合适的电缆包括：每条有四对双绞线的 UTP 电缆，每条有两对双绞线的 STP 电缆，62.5/125mm 光纤。不过现在应用最为广泛的还是 UTP。

要注意的是，双绞线的传输距离的限制是 100 米，而它包括信息插座到计算机的活动短线、水平子系统、配线架到集线器的跳线。最好不要使这三段线的总和超过 100 米。

在水平子系统中最常见的安装方法有两种：一种是暗管预埋、墙面引线（也就是走线于天花板）；另一种则是地下管槽，地面引线（也就是走线于地板下，通常会在有地毯或静电地板时采用）。可以根据实际情况来选择。

6）工作区子系统

工作区子系统所定义的范围涵盖了信息插座到工作站设备这部分相关的网络设备。它包含以下组件：工作站设备（如计算机、接收数据的终端机或电话等）、连接计算机的活动短线（包含了插座、连接到网卡的短线或是光纤的转接头）、网卡。

规划使用者工作区子系统的原则十分简单，主要是让使用者拥有更大的调整工作环境的自由，因此要尽量让这部分设备便于拆装、增减设备、调整位置，以符合不同工作的需求，而信息插座与线材的排列也要整齐划一，以便于管理和维护。

另外，应注意给每一条电缆、信息插座、配线架上注明清楚的编号，这样对于日后维护网络时检查线路会有很大的帮助。

【问题 2】

综合布线系统设计依据如下：

- 标准：IEEE 802.3 10Base-T，IEEE 802.3 100Base-Tx，100Base-Fx，IEEE 802.3 1000Base-Sx，1000Base-Lx，EIA/TIA 568EIA/TIA-TSB 36/40 工业标准，及国际商务建筑布线标准，ISO/IEC 11801，ISO/IEC JTC1/SC25/WG3，ANSI FDDI/TPDDI 100Mbps，CCITT ATTM155Mbps，CCITT ATM622Mbps。
- 安装与设计规范：中国建筑电气设计规范、工业企业通信设计规范、中国工程建设标准化协会标准“建筑与建筑群综合布线系统工程设计规范”、结构化布线系统设计总则、市内电话线路工程施工及验收技术规范。

从理论上讲，大型布线系统需要用铜介质和光纤介质部件，将六个子系统集成在一起考虑性能与价格因素：

- 建筑群子系统。采用多模光缆连接新、旧大楼，中心计算机房的主机及网络设备。
- 垂直干线子系统。垂直干线子系统提供建筑物的干线电缆，负责连接管理间子系统到设备间子系统的子系统。垂直干线子系统一般选用光缆，以提高传输速率。垂直干线电缆的拐弯处，不要直角拐弯，应有相当的弧度，以防止光缆受损。
- 水平子系统。将设备间子系统的线路延伸到用户工作区，数据部分和语音部分均采用 ISDN 增强型五类双绞线；水平子系统的作用是将主干子系统的线路延伸到用户工作区子系统。水平子系统的数据、图形等电子信息交换服务将采用 4 对超 5 类非屏蔽双绞线（Cat. 5 UTP）布线。超 5 类非屏蔽双绞线是目前性能价格比最好的高品质传输介质，其性能指标完全符合 ANSI/EIA/TIA-568 标准，能够保证在 100m 范围内传输率达到并超过 100Mbps。根据超 5 类 UTP 用于支持 100Mbps 传输的最大距离为 100m 的设计，设计线从配线架至最远端（工作区）的端口小于 90m。

水平子系统由 8 芯非屏蔽双绞线组成。常用的双绞线有 3 类线和超 5 类线。3 类线可用于电话和 16Mbps 的数据传输；超 5 类线传输数据的速度可达到 100Mbps。为适应以后扩展的要求，并最大限度地保护投资，应采用超 5 类线模式。

【问题 3】

每个工作区子系统中通常都有两个以上的信息插座，一个用于传输声音（电话线路），一个用来传输数据（电脑网络线路），这两种线路可以说是目前办公室必备的配置，也是目前最流行的信息整合网络，其实就是将办公室内所有的信息线路均整合在一起。信息插座的外观与内部结构如图 10-8 所示。

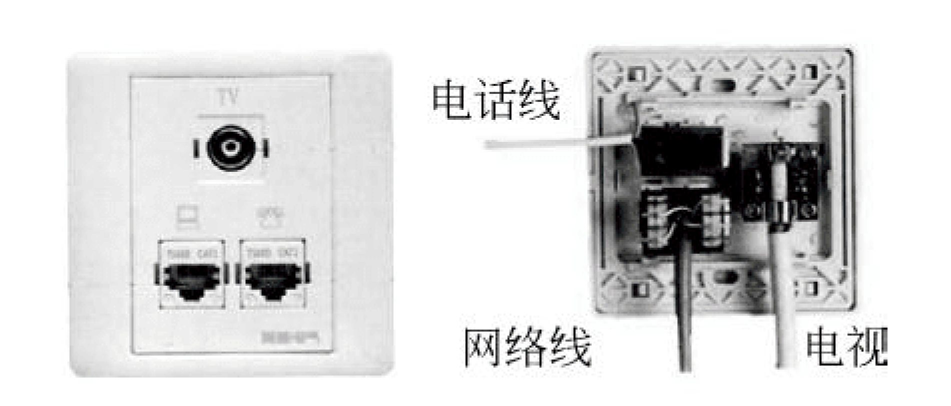


图 10-8　信息插座示意图

而现在的信息插座通常都将这两个接口（甚至三个接口）集成在一起。针对数据和语音都可以采用 MDVO 模块式超 5 类信息插座。为用户提供一个既符合标准，又可满足高速数据传输的标准。插座选用 8 芯 RJ-45 型。跳线用于连接插座与 PC。跳线的两端带 RJ-45 插头。也就是应该考虑配备双孔插座。计算机、电话可按用户的需要，随意跳接。

【问题 4】

理论上 UTP 的 4 对绞线都可以使用，为什么 TIA/EIA 还要硬性规定哪一种颜色的线要接到连接头的哪一个脚位上呢？其原因主要是以太网络只使用 1，2，3，6 这四条线，其中 1，2 与 3，6 各成一组，根据实验结果，每组线使用同一对双绞线，因其互相缠绕，可以大幅降低干扰。根据实验室测试的结果，按照这两种标准定义的排列方式所做的连接头，其电缆传输品质确实优于其他的排列方式，因此建议双绞线连接头各色线的排列方式如表 10-5 所示。

表 10-5　568A/568B 标准

连接头脚位	568A 定义的色线位置	568B 定义的色线位置
1 脚位	白绿（W-G）	白橙（W-O）
2 脚位	绿（G）	橙（O）
3 脚位	白橙（W-O）	白绿（W-G）
4 脚位	蓝（BL）	蓝（BL）
5 脚位	白蓝（W-BL）	白蓝（W-BL）
6 脚位	橙（O）	绿（G）
7 脚位	白棕（W-BR）	白棕（W-BR）
8 脚位	棕（BR）	棕（BR）

从表 10-5 中，我们可以发现，568A 与 568B 的差异主要是 1，2 与 3，6 两组绞线对调，其他的脚位是相同的。

如果想用双绞线直接连接两个同类型的网络器材，例如，Hub 对 Hub 或是网卡对网卡，这段电缆的 RJ-45 接头必须反跳（CrossOver，也称为交叉），也就是左端 1，2 对应到右端的 3，6，左端的 3，6 对应到右端的 1，2，其余不变。实际上，只需要记住一边用 568A，一边用 568B，就可以制作出一条交叉线了。

例题 2 答案

【问题 1】

（1）建筑群子系统（楼宇子系统）

（2）设备间子系统（机房子系统）

（3）干线子系统（垂直干线子系统）

（4）管理子系统（布线配线子系统）

（5）水平布线子系统

（6）工作区子系统（用户区子系统）

【问题 2】

（1）采用多模光缆或单模光缆。

（2）干线子系统可以根据速度需要进行选择，包括多模/单模光缆；5 类 UTP、超 5 类 UTP、6 类 UTP 等。

（4）采用超 5 类（5 类）UTP。

【问题 3】

应选择型号为 RJ-45，采用 8 芯接线，符合 IBDN 标准，满足高速数据传输的标准信息插座。而现在常使用多媒体信息模块式超五类信息插座。

【问题 4】

（1）白橙	（2）橙色	（3）白绿	（4）蓝色
（5）白蓝	（6）绿色	（7）白褐（白棕）	（8）褐色（棕色）

例题 3

某公司内部的网络的工作站采用 100Base-TX 标准与交换机相连，并经网关设备采用 NAT 技术共享同一公网 IP 地址接入互联网，如图 10-9 所示。

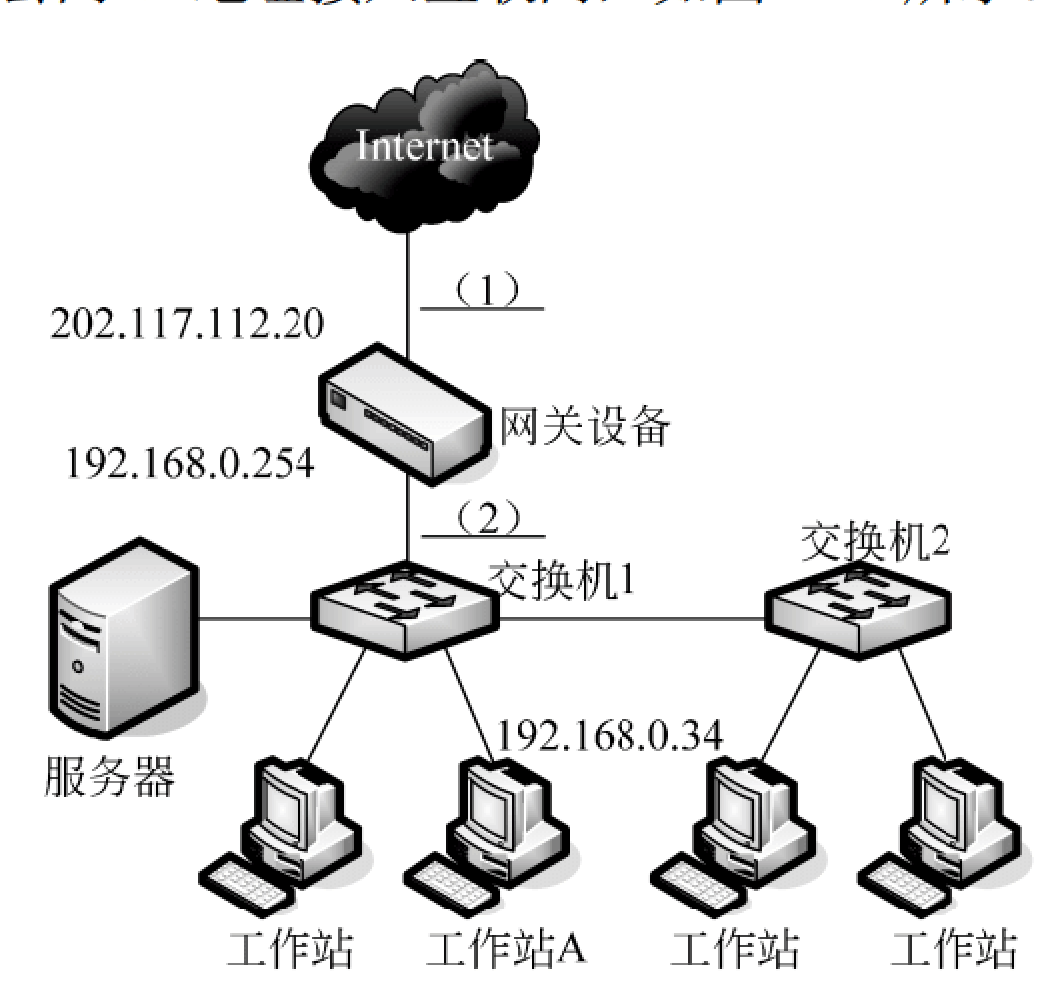


图 10-9　网络拓扑结构示意图

【问题 1】

连接交换机与工作站的传输介质是什么？介质需要做成直通线还是交叉线？最大长度限制为多少？

【问题 2】

交换机 1 与交换机 2 之间相距 20 米，采用交换机堆叠方式还是交换机级联方式？

【问题 3】

在工作站 A 的网络配置中，网关地址是什么？

【问题 4】

从以下备选答案中选择两种能够充当网关的网络设备。

备选答案：A. 路由器　　B. 集线器　　C. 代理服务器　　D. 网桥

【问题 5】

若工作站 A 访问外部 Web 服务器，发往 Internet 的 IP 包经由（1）和（2）处时源 IP 地址分别是什么？

例题 3 分析

【问题 1】

局域网有三种基本的拓扑结构：总线型、星型和环型。而星型拓扑通常是以集线器或交换机为中心组网的，采用的传输介质是无屏蔽双绞线（UTP）。双绞线分为直通线和交叉线两种类型：

（1）直通线。

对于用来将 PC 机、服务器连接到交换机、集线器等网络设备的双绞线，我们通常称其为直通线。直通线是连接网络时最常用的线缆类型，它两端的线序是完全一样的，均为 T568A 线序或 T568B 线序。

（2）交叉线。

如果你需要对交换机、集线器之间进行堆叠，或者直接用一根双绞线连接 2 台 PC，这时就需要使用交叉线。

在制作交叉线时，两端的 RJ-45 接头必须反跳（CrossOver，也称为交叉），也就是左端 1，2 对应到右端的 3，6，左端的 3，6 对应到右端的 1，2，其余不变。因此，我们可以在一端使用 T568A 线序，另一端使用 T568B 线序。

而每种线缆在传输信号时都可能衰减，因此都有最大长度的限制。屏蔽双绞线、非屏蔽双绞线的最大段长度都是 100 米，细同轴电缆的最大段长度是 185 米，粗同轴电缆的最大段长度是 500 米，光纤的最大段长度则可达 2000～5000 米。

【问题 2】

堆叠和级联是扩展交换机端口的两种常用方法。堆叠需要通过厂家提供的专用连接电缆（其长度一般不超过 2 米），它通常不会占用集线器上原有的普通端口，但需要交换机能够支持堆叠。

级联则是通过普通的端口、普通的双绞线（最大长度是 100 米）完成集线器连接的。在具体连接时有两种方式：一种是使用直通线连接集线器的 UPLink 端口；另一种是使用交叉线连接集线器的普通端口。

【问题 3】

在图 10-9 中可知，整个局域网是通过网关设备连接 Internet 的，因此局域网中所有

工作站的网关都应该设置成该网关设备的 IP 地址，而该网关设备的局域网地址应该是192.168.0.254。

【问题 4】

在本题中的网关设备将实现两个不同逻辑子网连接，因此应该使用网络层以上的设备。而集线器工作在物理层，网桥工作在数据链路层，显然是无法实现的。而路由器和代理服务器都能够充当此处的网关设备。

【问题 5】

作为实现局域网接入 Internet 的网关设备，在此还将完成地址转换的工作，位置（2）处于局域网内，还没有经过 NAT 转换，因此从工作站 A 发送的数据包其源 IP 地址应该就是工作站 A 的 IP 地址 192.168.0.34。而位置（1）则已经到了外网，对于外网而言局域网中的地址是不可见的，因此源 IP 地址就将改为网关设备的外网地址，即应该是202.117.112.20。

例题 3 答案

【问题 1】

连接交换机与工作站的传输介质是双绞线，应使用直通线，最大长度为 100 米。

【问题 2】

交换机级联方式。

【问题 3】

192.168.0.254

【问题 4】

A，C

【问题 5】

在（1）处时源 IP 地址是 202.117.112.20，到（2）处时源 IP 地址是 192.168.0.34。

例题 4

基于 MAC 地址划分 VLAN 的优点是<u>（1）</u>。

（1）A．主机接入位置变动时无需重新配置

B．交换运行效率高

C．可以根据协议类型来区分 VLAN

D．适合于大型局域网管理

例题 4 分析

基于 MAC 地址划分 VLAN 的方法是根据每个主机的 MAC 地址来划分，即对每个 MAC 地址的主机都配置它属于哪个组，它实现的机制就是每一块网卡都对应唯一的 MAC 地址，VLAN 交换机跟踪属于 VLAN MAC 的地址。这种方式的 VLAN 允许网络用户从一个物理位置移动到另一个物理位置时，自动保留其所属 VLAN 的成员身份。

由这种划分的机制可以看出，这种 VLAN 的划分方法的最大优点就是当用户物理位

置移动时，即从一个交换机换到其他的交换机时，VLAN 不用重新配置，因为它是基于用户，而不是基于交换机的端口。这种方法的缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置是非常累的，所以这种划分方法通常适用于小型局域网。而且这种划分的方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，保存了许多用户的 MAC 地址，查询起来相当不容易。

例题 4 答案

（1）A

例题 5

下面有关 VLAN 的说法正确的是__（2）__。

（2）A．一个 VLAN 组成一个广播域　　B．一个 VLAN 是一个冲突域

C．各个 VLAN 之间不能通信　　D．VLAN 之间必须通过服务器交换信息

例题 5 分析

冲突域（物理分段）：连接在同一导线上的所有工作站的集合，或者说是同一物理网段上所有节点的集合或以太网上竞争同一带宽的节点集合。这个域代表了冲突在其中发生并传播的区域，这个区域可以被认为是共享段。在 OSI 模型中，冲突域被看作是第一层的概念，连接同一冲突域的设备有 Hub，Repeater 或者其他进行简单复制信号的设备。也就是说，用 Hub 或者 Repeater 连接的所有节点可以被认为是在同一个冲突域内，它不会划分冲突域。而第二层设备（网桥，交换机）第三层设备（路由器）都可以划分冲突域的，当然也可以连接不同的冲突域。简单地说，可以将 Repeater 等看成是一根电缆，而将网桥等看成是一束电缆。

广播域：接收同样广播消息的节点的集合。如：在该集合中的任何一个节点传输一个广播帧，则所有其他能收到这个帧的节点都被认为是该广播帧的一部分。由于许多设备都极易产生广播，所以如果不维护，就会消耗大量的带宽，降低网络的效率。由于广播域被认为是 OSI 中的第二层概念，所以像 Hub，交换机等第一，第二层设备连接的节点被认为都是在同一个广播域。而路由器，第三层交换机则可以划分广播域，即可以连接不同的广播域。注：一个 VLAN 是一个广播域，VLAN 可以隔离广播，划分 VLAN 的其中的一个目的就是隔离广播。

例题 5 答案

（2）A

例题 6

可在提高 Web 服务器响应性能的同时，增加可靠性的措施是__（3）__。

（3）A．增加网络带宽

B．搭建多个服务器的集群

C．服务器安装高版本操作系统

D．提高服务器的硬盘速率

例题 6 分析

增加网络带宽、搭建多个服务器的集群、服务器安装高版本操作系统、提高服务器的硬盘速率都能提高 Web 服务器响应性能。但是增加网络带宽、提高服务器的硬盘速率为提升硬件性能，并不能明显的提高可靠性。而服务器安装高版本操作系统，也许只是应用功能的完善。搭建多个服务器的集群，则编外多台机器响应 Web 服务，因此可靠性大大加大了。

例题 6 答案

（3）C

第 11 章　网络设备的配置

根据 09 版考试大纲，本章要求考生掌握交换机和路由器的基本配置。

希赛教育专家特别提示：新增加的内容重点考查的内容将为 VLAN 配置、路由器路由协议配置等几方面的知识。这无疑对网络管理员们提出了更高的要求。

11.1　交换机的配置

交换机工作在 OSI 第二层，即数据链路层设备，网络管理员考试对交换机配置的考查，比较明朗、清晰。主要考查的是交换机的基础配置（几种工作模式、IP 地址信息的配置）和 VLAN 的管理配置，其中 VLAN 所涉及的两个协议 VTP 和 STP 协议将作为考试的考点，在本节中做了详细介绍。本节将结合相关实例，对在同一交换机上配置 VLAN 或跨越交换机创建 VLAN 的配置过程。

11.1.1　交换机的基本配置

交换机有多种配置方式，各种方式又有不同的区别：

（1）用 Console 线缆把配置主机直接连接到 Console 口进行配置。即用控制线连接计算机的 COM1 口和交换机的 Console 口，再进行计算机的“超级终端”环境进行配置。

（2）通过网络上的终端运行终端仿真软件进行远程配置。即通过交换机的 AUX 口连接 Modem，再通过电话线与互联网连接，网络终端通过 Telnet 远程登录进行配置。

（3）通过 Telnet 程序进行远程配置，这需要接入方必须知道该交换机的 IP 地址，因此，在初始化配置中，这种方法是行不通的。

（4）通过 IE 浏览器来访问，这只在交换机内置了 Web 用户界面才可使用，也需要 IP，不能用于初始配置。

（5）通过专用的网管软件，比如用 CiscoWork 来对 Cisco 的交换机进行管理配置。

一般在配置过程中采用第一种方式，运用 Windows 系统中自带的“超级终端”进行配置。接口与线缆连接成功后，开启交换机电源，启动“超级终端”，并配置如下参数：

端口速率：9600bps；

数据位：8；

奇偶校验：无；

停止位：1；

数据流控制：无。

11.1.2　配置模式状态

交换机有以下几种配置模式：

（1）用户模式：登录到交换机时会自动进入用户模式，提示符为：Switch>。在该模式下，只能够查看相关信息，对 IOS 的运行不会产生任何影响。

（2）特权模式：用户模式下，键入 enable 命令，即可进入特权模式，提示符为：Switch#。该模式下可以完成任何操作，包括检查配置文件，重启交换机等，它的命令集是用户模式下的超集。

（3）全局配置模式：特权模式下，键入 config terminal 命令，即可进入全局配置模式，提示符为：Switch（config）#。该模式下可以完成如 VLAN 的划分等影响 IOS 的全局操作。

（4）局部（子）配置模式：全局模式下，键入特定子模式命令（如 interface ethernet0/1），即可进入以太网端口配置模式，提示符为：Switch（config-XX）#。该模式用于单独对组件、端口、进程等进行配置。

11.1.3　交换机配置命令

交换机的基本配置主要包括口令与主机名设置、IP 地址与网关设置、端口参数设置及一些其他常用命令。

1．口令与主机名设置

```
Switch> enable                          # 用户模式提示符下键入 enable 命令
Switch#                                 # 进入特权模式
Switch# config terminal                 # 特权模式提示符下键入命令
Switch(config)#                         # 进入全局配置模式
Switch(config)# enable password test    # 设置口令为 test
Switch(config)# enable secret test2     # 设置加密口令为 test2
Switch(config)# hostname CSAI           # 设置交换机名为 CSAI
CSAI(config)# end                       # 退回特权模式
```

注意：enable password 与 enable secret 只要配置一项即可，两者若都配置，后配置生效。它们的区别在于，前者在配置项中是以明文显示，而后者是以密文显示。

2．IP 地址与网关设置

```
CSAI(config)# ip address 192.168.0.1 255.255.255.0  # 设置交换机 IP 地址
CSAI(cconfig)# ip default-gateway 192.168.0.1       # 设置交换机默认网关
```

3．端口参数设置

```
CSAI(config)# interface fastethernet0/1 # 进入交换机第 0 槽的第一个快速以太网
                                          端口的子模式
CSAI(config—if)# speed 10|100|auto      #设置端口速率，可选项为：10M，100M，
                                         auto(自适应)
```

```
CSAI(config—if)# duplex half|full|auto # 设置端口速率，可选项为：半双工，全
                                          双工，auto(自动)
```

4．其他常用命令

除上述命令外，交换机还有一些其他的配置命令，如表 11-1 所示。

表 11-1　其他常用命令

命　　令	描　　述
Show run	显示交换机的运行配置
shutdown /No shutdown	关闭/启用某个接口
Set prompt name	设置提示符
Set interface sc0 ip-addr sub-mask	设置交换机的管理口 IP 信息
Show config	显示交换机的当前配置

11.2　VLAN 基本配置

VLAN 技术是交换技术的重要组成部分，也是交换机的重要进步之一。它把物理上直接相连的网络从逻辑上划分多个子网。每一个 VLAN 对应一个广播域，处于不同 VLAN 上的主机不能进行通信，不同 VLAN 之间的通信要引入第三层交换技术才可以解决。对虚拟局域网的配置管理主要涉及到静态 VLAN 配置、VTP 协议和 STP 协议的配置。

1．静态 VLAN 配置

静态 VLAN 划分也被称为基于端口的 VLAN 划分，其基本配置命令如表 11-2 所示。

表 11-2　静态 VLAN 配置过程

配 置 步 骤	命　　令	注　　释
1．准备工作	vlan database	进入 vlan 配置子模式
2．创建 Vlan	vlan 2	创建一个 vlan2
3．为 Vlan 创建别名	vlan 2 name Vcsai	将一个编号为 2 的 vlan 命名为 Vcsai
4．将端口划入 Vlan	Interface f0/9 Switchport mode access switchport access vlan 2	把端口 9 分配给 Vlan2

2．配置 VTP 协议

VTP（VLAN Trunking Protocol，VLAN 中继协议）通过网络保持 VLAN 配置统一性。VTP 在系统级管理、增加、删除、调整 VLAN，自动地将新的 VLAN 信息向网络中其他的交换机广播。此外，VTP 减小了那些可能导致安全问题的配置。两交换机间的连线，称之为 Trunk。

1）相关概念

- VTP 模式：当交换机配置在 VTP Server 或透明模式时，可以使用 CLI、控制台菜

单、MIB 修改 VLAN 配置。

- VTP Domain：交换 VTP 更新信息的所有交换机必须配置为相同的管理域。
- ISL：（inter-switch link）是由 Cisco 公司开发的私有技术，在帧的前面和后面都添加封装信息，其中包含了 VLAN ID。是一个在交换机之间、交换机与路由器之间及交换机与服务器之间传递多个 VLAN 信息及 VLAN 数据流的协议，Cisco 交换机的专用。
- IEEE 802.1Q 标准：IEEE 制定的用于识别在中继链路上识别数据帧技术，它通过在帧头插入一个 VLAN 标识符来标识 VLAN，通常称为“帧标记”，以标识数据帧来自哪个 VLAN。交换机会读懂该标识并作出相应的操作。当数据帧离开干道时，该标识被去除。数据帧的标记是在 OSI 参考模型中的第二层上的操作，对交换机的开销较小。由于是 IEEE 制定的，所以各个厂商的交换机基本都支持该标准。
- Trunk：在路由与交换领域，Trunk 是指 VLAN 的端口聚合，用来在不同的交换机之间进行连接，以保证在跨越多个交换机上建立的同一个 VLAN 的成员能够相互通信。

正如网络中也存在主机与服务器一样，应用 VTP 的交换机也分三种不同的工作模式：

- 服务器模式：它负责定义 VLAN 信息，并广播传输给其他交换机。
- 客户端模式：接收并使用来自服务器端发送过来的 VLAN 信息。
- 透明模式：接收并转发来自服务器端发送过来的 VLAN 信息，但自己并不应用，是交换机的默认工作模式。

```
switch# vlan database                          # 进入 VLAN 配置子模式
switch(vlan)# vtp client|server|transparent    # 设置交换机工作模式
```

2）VTP 协议配置过程

VTP 协议的相关配置，参考表 11-3。

表 11-3　VTP 协议配置过程

配 置 步 骤	命令及命令注释	说　　明
1．设置 VTP domain	vlan database　　# 进入 vlan 配置模式 vtp domain vname # 设置 vtp 管理域名称 vtp server | client　# 设置交换机为服务器（或客户端）模式	vtp domain 称为管理域，交换 vtp 更新信息的所有交换机必须配置为相同的管理域。核心交换机和分支交换机都要配置
2．启用修剪功能	vlan pruning　　# 启用修剪	减少不必要的数据流量，充分利用带宽
3．配置中继	interface fa0/1 switchport trunk encapsulation isl | dot1q # 封装中继协议 switchport mode trunk # 端口设置为中继模式 switchport trunk allowed vlan vlan-list | all	核心交换机上以上都要配置，先进入交换机端口模式，再封装中继协议，配置端口中继模式。 vlan-list | all 是允许所有或部分 VLAN 信息通过 trunk 链路

3．生成树协议 STP 配置

生成树协议是交换式以太网中重要的概念和技术，该协议的目的就是在实现交换机之间的冗余连接的同时，避免网络环路的出现，实现网络的高可靠性。它通过在交换机之间传递桥接协议数据单元（Bridge Protocol Date Unit，BPDU）来相互告知诸如交换机的桥 ID、链路性质、根桥（Root Bridge）ID 等信息，以确定根桥，决定哪些端口处于转发状态，哪些端口处于阻断状态，以免引起网络环路。

生成树协议 STP 的主要配置命令如下：

调整根路径成本：

```
switch(config-if)# spanning-tree [vlan vlan-list] cost cost
```

调整端口 ID：

```
switch(config-if)# spanning-tree [vlan vlan-list] port-priority
port-priority
```

端口权值默认为 128，数字越小，优先级越高。

修改 STP 时钟：

```
switch(config)# spanning-tree [vlan vlan-list] hello-time seconds
switch(config)# spanning-tree [vlan vlan-list] forward-time seconds
switch(config)# spanning-tree [vlan vlan-list] max-age seconds
```

11.3 路由器的配置

路由器是 Internet 的核心设备，也是网络互联的最主要的设备，因此深入了解路由器的基本概念，熟悉常见的配置方法是十分重要的。根据 09 版大纲的要求，重点在于路由器的选择协议方面。会以大题形式出现，希赛教育专家特别提示，上午模块对本节的考查目标主要在对各种路由协议的概念、实现方法的理解。因此考生不仅要注重实践配置，还要对理论有深入的了解、辨别能力。

11.3.1 路由器的基本配置

本知识点主要在于了解路由器的作用、特点、组成以及四种不同的配置模式，掌握访问路由器的方法，以及路由器的基本配置方法。

路由器是一种典型的网络层设备，在 OSI 参考模型中完成网络层中继或第三层中继的任务。路由器负责在两个局域网的网络层间传输数据分组，并确定网络上数据传送的最佳路径（选路协议、路由选择协议）。

1．访问路由器

访问路由器与访问交换机一样，可以通过 Console（控制台）端口连接终端或安装

了终端仿真软件的 PC（第一次访问时必须采用），通过设备 AUX 端口连接 Modem；通过 Telnet，通过浏览器，以及通过网管软件五种方式进行访问。

而使用 Console 端口连接的方式，通常也是使用“超级终端”仿真软件，并将端口的属性配置为：端口速率为 9600bps，数据位为 8，奇偶校验无，停止位为 1，流控无。

2．路由器的组成

与交换机一样，Cisco 路由器也有 4 种功能不同、材质不同的内存，用来存储引导软件的 ROM，用来保存 IOS 系统软件的 Flash，用来作为主存的 RAM，用来保存启动配置的 NVRAM。

在路由器中，包括两份配置。一份是当前运行的（running-config），存储在 RAM 中的，表示为路由器当前生效的配置参数；另一份则是备份配置（start-config），存储在 NVRAM 中，每次启动时会自动装入。

3．配置状态与转换命令

与交换机一样，Cisco 路由器也分为用户模式（登录时自动进入，只能够查看简单的信息）、特权模式（也称为 EXEC 模式，能够完成配置修改、重启等工作）、全局配置模式（对会影响 IOS 全局运作的配置项进行设置）、子配置模式（对具体的组件，如网络接口等进行配置）。四种状态的转换命令如图 11-1 所示。

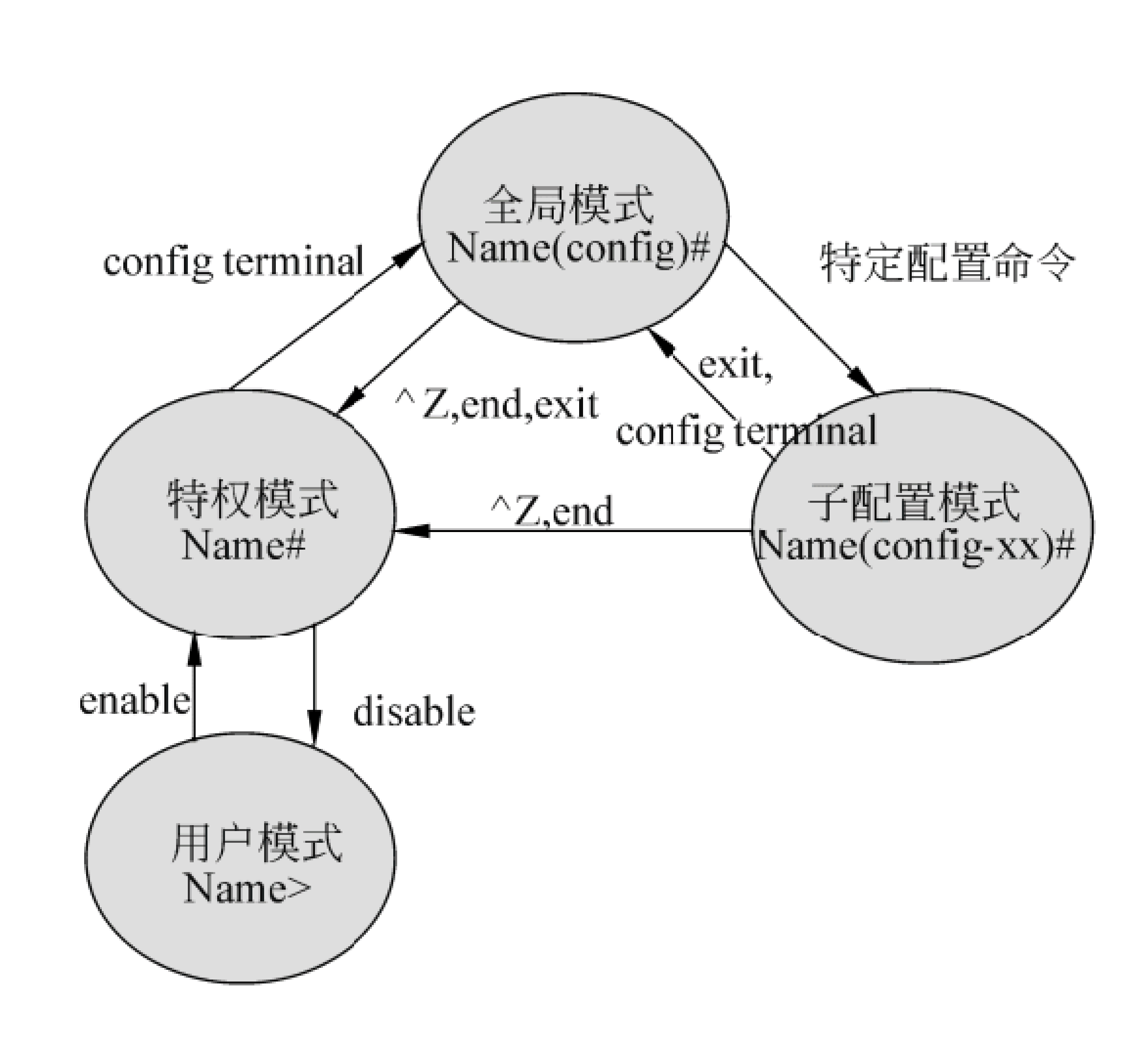


图 11-1　Cisco 路由器配置状态转换图

4．路由器基本配置

1）配置 enable 口令和主机名

```
Router>                                   （用户模式提示符）
Router> enable                            （进入特权模式）
Router #                                  （特权模式提示符）
```

```
Router # config terminal                     （进入配置模式）
Router (config) #                            （配置模式提示符）
Router (config) # enable password test       （设置 enable 口令为 test）
Router (config) # enable secret test2        （设置 enable 加密口令为 test2）
Router (config) # hostname R1                （设置主机名为 R1）
Router (config) # end                        （退回特权模式）
R1#
```

注：enable password 和 enable secret 只要配置一个就好，两者同时配置后者生效。它们的区别在于，enable password 在配置项中是明文显示，而 enable secret 是密文显示。

2）接口基本配置

在 Cisco 路由器中通常是模块化的，每个模块都有一些相应的接口，例如以太网口、快速以太网口、串行口（serial，即广域网口）等。而且与交换机不同，它们在默认情况下是关闭的，需要人为启动它。

```
Router> enable                               （进入特权模式）
Router # config terminal                     （进入全局配置模式）
Router (config) # interface fastethernet0/1  （进入接口 F0/1 子配置模式）
Router (config-if) # ip address 192.168.0.1 255.255.255.0
                                             （设置该接口的 IP 地址）
Router (config-if) # no shutdown             （激活接口）
11:02:01:%LINK-3-UPDOWN:Interface FastEthernet 0/1 changed state to up.
Router (config-if) # end                     （退回到特权模式）
```

11.3.2 路由技术与路由协议

本知识点在于了解两大类四种主要路由选择技术的特点与适用点，了解 RIP、IGRP、OSPF、EIGRP 四种主要路由选择协议的特点，掌握它们的配置技术，深入掌握 RIP、IGRP 等路由选择协议的更新汇聚问题。

1．路由应用范围

根据路由选择协议的应用范围，可以将其分为内部网关协议、外部网关协议和核心网关协议三大类。其分类如图 11-2 所示。

（1）自治系统：是指同构型的网关连接的互联网络，通常是由一个网络管理中心控制的。

（2）内部网关协议（IGP）：在一个自治系统内运行的路由选择协议，主要包括 RIP、OSPF、IGRP、EIGRP 等。

（3）外部网关协议（EGP）：是指在两个自治系统之间使用的路由选择协议，最新的 EGP 协议是 BGP，其主要的功能是控制路由策略。

边界网关协议（BGP）是运行于 TCP 上的一种自治系统间路由协议。BGP 是唯一设计来处理因特网的大小的协议，也是唯一能够妥善处理好非路由主机多路连接的协议。BGP 交互系统的主要功能是和其他的 BGP 系统交换网络可达信息。网络可达信息包括可达信息经过的自治系统（AS）清单上的信息。这些信息有效地构造了 AS 互联并由此清除了路由环路，同时在 AS 级别上实施了策略决策。

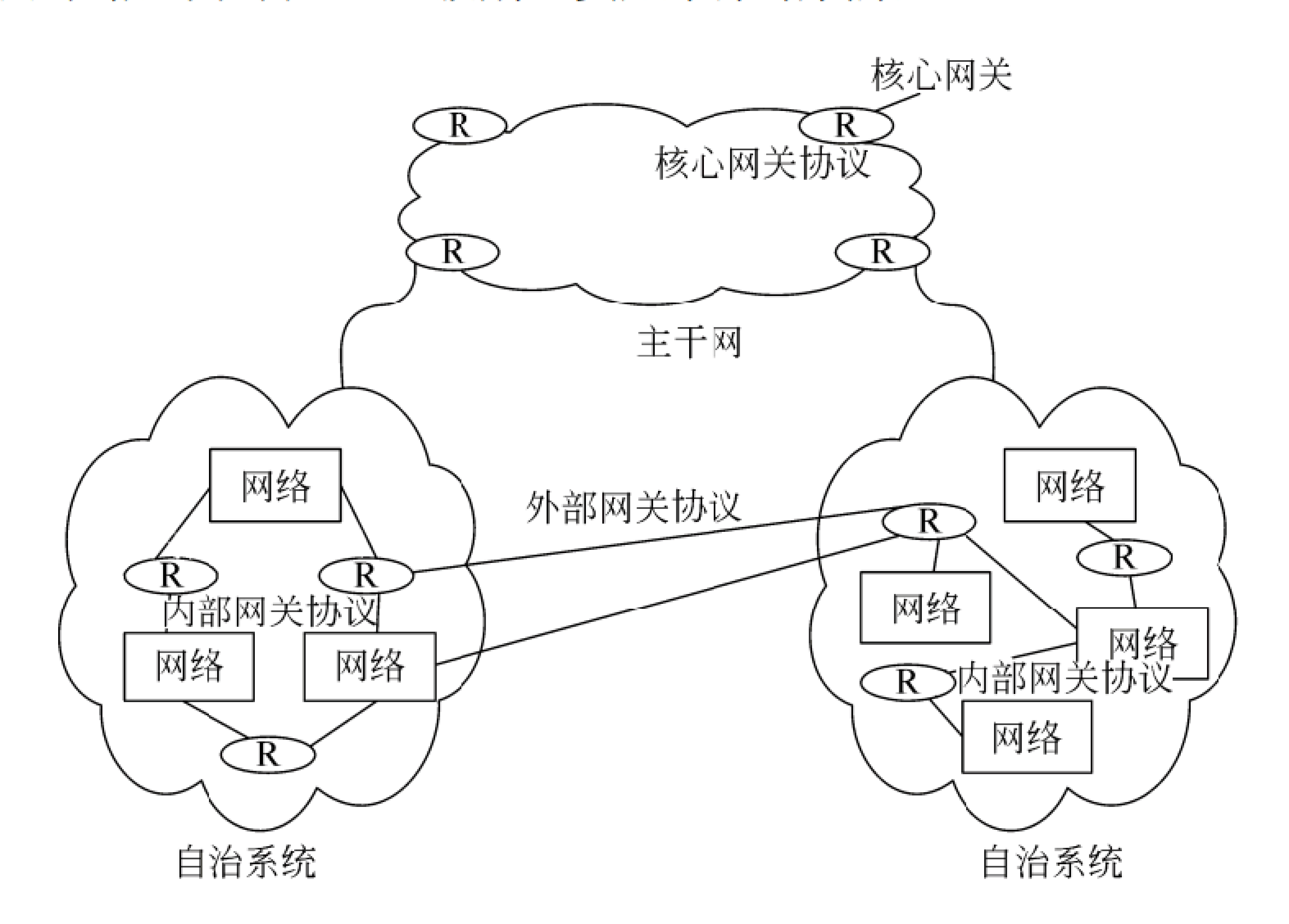


图 11-2　路由选择协议的应用范围

BGP 特点如下：

- 距离矢量协议。
- 传输协议：TCP，端口号：17。
- 支持 CIDR（无类别域间选路）。
- 路由更新只发送增量路由。
- 丰富的路由过滤和路由策略。

我们常接触、使用得较多的路由选择协议是内部网关协议，根据算法的不同，主要包括 RIP、OSPF（开放最短路径优先）、IGRP（内部网关路由协议）、EIGRP（增强型内部网关路由协议）、IS-IS 五种。路由选择协议将路由信息发送到其他节点所采用的基本算法是扩散法，为了避免信息重复发送，通常会对路由信息包进行编号，通常是每发送一个路由信息就递增编号（即加 1）。表 11-4 中总结了五种常见路由协议的知识点。

表 11-4　路由协议比较

协　议	类　别	主 要 特 点
RIP	距离向量协议	使用广泛，简单、可靠，支持 CIDR、VLSM 及连续子网，最大跳数是 15（隔一个路由器为一跳），每隔 30 秒广播一次路由信息。但其收敛慢，网络规模受限

续表

协　议	类　别	主 要 特 点
IGRP	距离向量协议	使用组合用户配置尺度（包括延时、带宽、可靠性、负载），不支持 VLSM 和不连续子网，每 90 秒发送一次路由更新广播
OSPF	链路状态协议	通过路由器间通告网络接口状态（使用 LSA——链路状态通告）来建立链路状态数据库，生成最短路径树，每个路由器自己构造路由表。使用 Dijkstra 算法。主要优点是：迅速、无环路的收敛性、支持精确度量，但路由开销大
EIGRP	平衡混合（前两种）	使用一种散射更新算法，实现很高的路由性能。支持 VLSM、不连续子网，支持自动路由汇总功能，支持多种网络层协议
IS-IS	链路状态协议	能够应用于内部网关，也可用于外部网关

2．路由协议分类

路由器可以使用两种基本方式进行路由选择：一是使用预先设置好的静态路由；二是使用一种动态路由选择协议来动态地计算路由。而动态路由选择协议根据实现机制的不同，又可以分为距离矢量路由选择、链路状态路由选择和混合路由选择三种类型。

1）静态路由

静态路由是预先设置的，将发现和传播路由的工作交给了互联网络管理者。

优点：有利于更安全的网络，能够更充分地利用资源，可以使用更小、更便宜的路由器。

缺点：当网络出现问题或其他原因引起拓扑变化时，需要管理员手工调整这些变化，在调整之前会因为无法识别失效的链路而造成路由失效。

适用场合：非常小、到给定目标只有一条路径的网络；大型或复杂网络中的一个安全局部。

2）距离矢量路由

距离矢量路由定期给直接相邻的网络邻居传送它们路由选择表的副本，每个接收者将一个距离矢量（就是它自己的距离“值”）加到表中，并转发给它的邻居，以形成对网络“距离”的累积透视图。距离矢量路由主要包括 RIP、IGRP 两种。

优点：协议简单，易于配置、维护与使用。

缺点：当网络出现问题或其他原因引起拓扑变化时，路由器要花一定的时间来“汇聚”对新网络拓扑的认知，在这个过程中可能出现错误的问题。

适用场合：适合于非常小的网络，这些网络没有或者有很少冗余路径，并且没有严格的网络性能要求。

3）链路状态路由

链路状态路由支持关于网络拓扑结构的复杂数据库，通过与网络中其他路由器交换链路状态通知来实现。而且链路状态的交换是由网络中的一个事件触发的，而不是定期进行的，这样就可以加快汇聚的过程。链路状态路由主要包括 OSPF。

优点：具有良好的灵活性、扩展性。

缺点：在初始的发现过程中，有可能产生路由交换的泛滥，从而降低网络性能；并且对内存和处理器的要求高，使得路由器的费用提高。

适用场合：适合任意大小的网络。

4）混合路由

混合路由主要包括 EIGRP，综合了距离矢量路由和链路状态路由的优点。

11.3.3　静态路由配置

所谓静态路由配置，也就是用户人为地指定对某一网络访问时所要经过的路径。在图 11-3 中则列出了一个静态路由配置的例子。

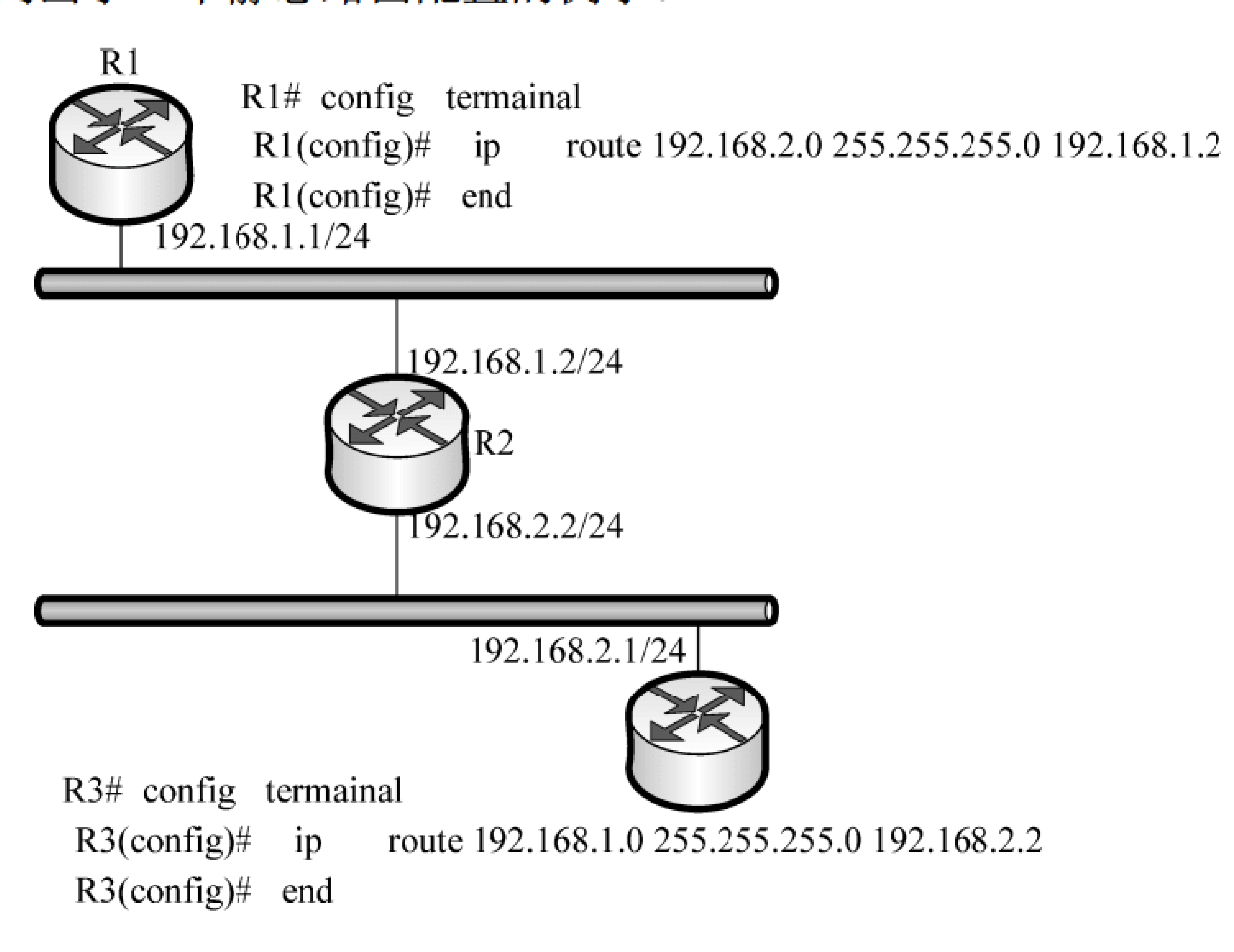


图 11-3　静态路由配置实例

其中最关键的配置语句是：

```
Router> ip route ip-addr subnet-mask gateway
```

ip-addr 为 IP 地址，subnet-mask 为子网掩码，gateway 为网关。其中 IP 地址指的是目标网络的地址，而网关处的 IP 地址则说明了路由的下一站。

11.3.4　RIP 协议配置

RIP 采用距离矢量算法（常常归于 Bellman-Ford 或 Ford-Fulkerson 算法）计算路由，是最早的路由选择协议之一。RIPv2 还支持 CIDR（无类域间路由）和 VLSM（可变长子网掩码），它只适用于小型的同构网络，它是以跳数表示距离的（每经过一个路由器则跳数加 1），允许的最大跳数为 15，因此任何超过 15 个中间站点的目的地均被表示为不可

达。RIP 是定期更新路由表的，它每隔 30s 广播一次路由信息。

1．RIP 路由配置常用命令

RIP 路由配置常用命令如表 11-5 所示。

表 11-5　RIP 路由配置常用命令

命　　令	说　　明
router rip	指定使用 RIP 协议
version {1|2}	指定 RIP 协议版本
network network-addr	指定与该路由器直接相连的网络
show ip route	查看路由表信息
Show ip route rip	查看 RIP 协议路由信息

2．RIP 配置实例

下面我们介绍一个网络的实例。

4 个位于不同地理位置的子网通过远程电缆连接在一起，现在要求使用 RIP 协议完成整个路由选择的配置，如图 11-4 所示。

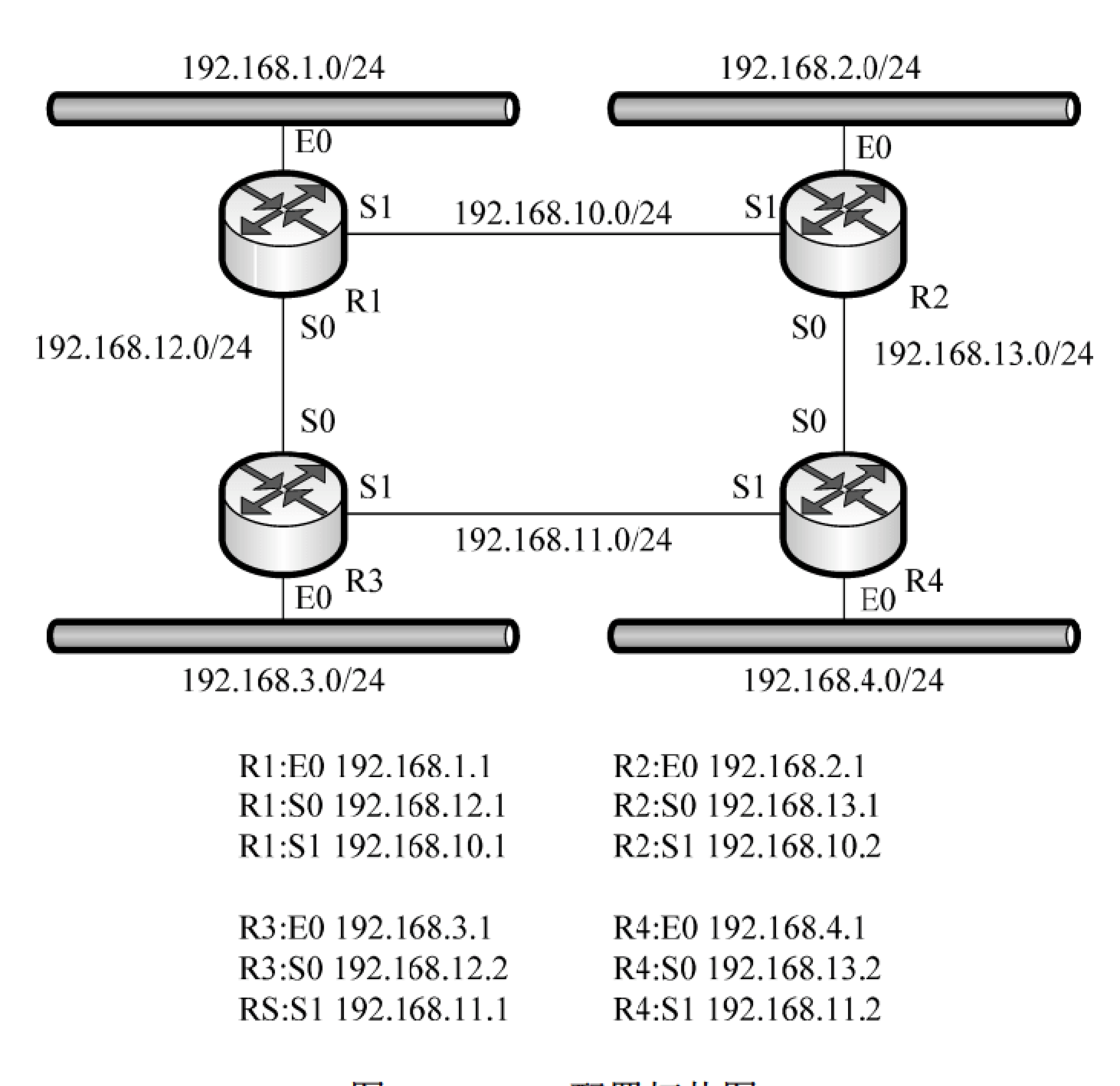


图 11-4　RIP 配置拓扑图

```
R1# config terminal                              (进入全局配置模式)
R1(config)# router rip                           (进入 RIP 协议配置子模式)
R1(config-router)# network 192.168.1.0           (说明路由器 R1 与 192.168.1.0 邻接)
R1(config-router)# network 192.168.10.0          (说明路由器 R1 与 192.168.10.0 邻接)
```

```
R1(config-router)# network 192.168.12.0 （说明路由器R1与192.168.12.0邻接）
R1(config-router)# version 2            （设置RIP的版本为2）
```

其他三个路由器的配置与此类似，只是根据其邻接网络的不同，修改相应的 network 子句即可。例如，路由器 R2 邻接的网络则是：192.168.2.0、192.168.10.0、192.168.13.0。

3．读懂 RIP 协议路由信息

当完成了 RIP 路由选择协议的配置之后，可以使用 show ip route 命令来查看路由表的信息。根据前面的配置，当查看 R1 的路由表时，将看到以下信息：

```
C    192.168.1.0   is directly connected,Ethernet0
C    192.168.12.0  is directly connected,Serial0
C    192.168.10.0  is directly connected,Serial1
R    192.168.2.0   [120/1] via 192.168.10.2, xx:xx:xx, Serial1
R    192.168.13.0  [120/1] via 192.168.10.2, xx:xx:xx, Serial1
R    192.168.3.0   [120/1] via 192.168.12.2, xx:xx:xx, Serial0
R    192.168.11.0  [120/1] via 192.168.12.2, xx:xx:xx, Serial0
R    192.168.4.0   [120/2] via 192.168.10.2, xx:xx:xx, Serial1
                   [120/2] via 192.168.12.2, xx:xx:xx, Serial0
```

第一部分，即最前面的 C 或 R 代表路由项的类别，C 是直连，R 代表是 RIP 协议生成的。

第二部分是目的网段。“[120/1]”表示 RIP 协议的管理距离为 120，1 则是路由的度量值，即跳数。可以看到路由器 R1 到 192.168.4.0 需要经过→R2→R4 或→R3→R4 两站，因此其度量值为 2，即两跳。

注：管理距离是用来表示路由协议的优先级的，RIP 的值为 120，OSPF 为 110，IGRP 为 100，EIGRP 为 90，静态设置为 1，直接连接为 0；因此我们可以看出在路由项中，EIGRP 是首选的，然后才是 IGRP，OSPF，RIP。

第三部分表示下一跳点的 IP 地址。

第四部分（xx:xx:xx）说明了路由产生的时间。

第五部分表示该条路由所使用的接口。

11.3.5　IGRP 协议配置

IGRP 与 RIP 之间最关键的区别在于度量值、路由确定算法及默认网关的使用。IGRP 在默认情况下是 90s 发送一次路由更新广播，在三个更新周期内（即 270s）没有从路由表中的一个路由器接收到更新，则会宣告路由不可访问。七个更新周期（即 630s）后，将清除该路由项。

1．IGRP 路由配置常用命令

IGRP 路由配置的常用命令如表 11-6 所示。

表 11-6 IGRP 路由配置的常用命令

命　　令	说　　明
router igrp autonomous-system	指定使用 IGRP 协议，其中 autonomous-system 是自治系统号，IGRP 协议只在相同自治系统号的路由器之间完成路由更新
network network-addr	指定与该路由器直接相连的网络
bandwidth 带宽	指定链路的带宽，通常单位为 Kbps
clockrate 时钟频率	指定链路的时钟频率，通常单位为 Hz
timer basic 更新周期 到期时间 抑制与否 清除时间	用来设置自定义的路由更新时间。例如，将更新时间缩短为 30s：timer basic 30 90 0 210
no metric holddown	禁止抑制功能，路由信息删除后可立即接收新的
metric maximum-hop 50	当信息包穿过 50 个路由器时，删除信息包

2．IGRP 配置实例

当网络的拓扑结构不确定、复杂时，利用 IGRP 路由选择协议可以根据延迟、带宽、可靠性和负载来进行优化，但其不支持 VLSM。如图 11-5 所示的就是一个 IGRP 的配置实例。

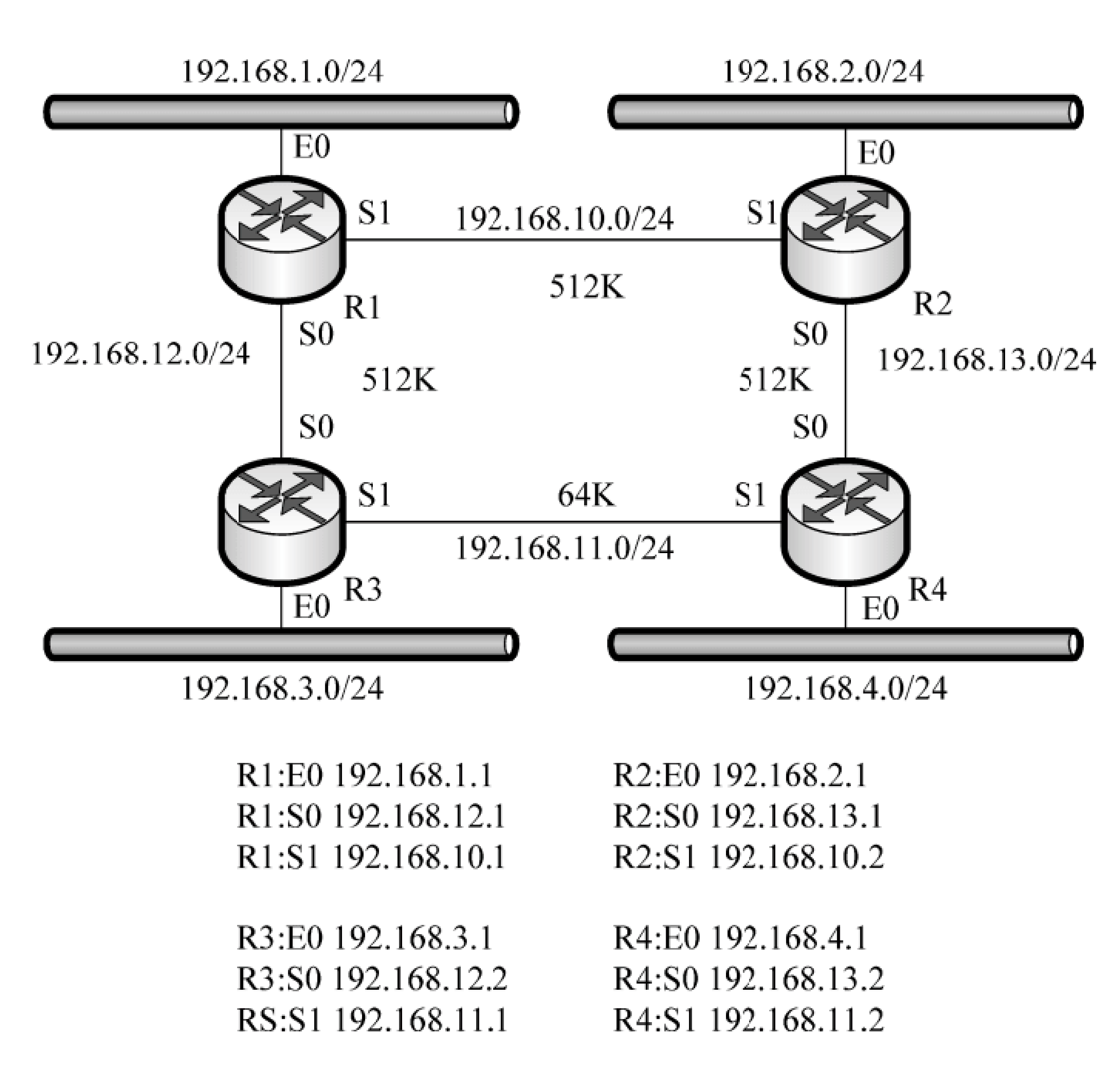


图 11-5 IGRP 配置拓扑图

下面以路由器 R3 为例，说明其配置的过程。

```
R3# config terminal                        （进入全局配置模式）
R3(config)# interface Ethernet0            （进入以太网口 0 子配置模式）
```

```
R3(config- if)# ip address 192.168.3.1 255.255.255.0  (配置 IP 地址)
R3(config- if)# no keepalive (不监测 keepalive 信号，即不连接设备时可激活该接口)
R3(config- if)# exit
R3(config)# interface Serial0                   (进入广域网口 0 子配置模式)
R3(config- if)# ip address 192.168.12.2 255.255.255.0 (配置 IP 地址)
R3(config- if)# bankwidth 512                   (设置带宽)
R3(config- if)# clockrate 512000                (设置时钟频率)
R3(config- if)# exit
R3(config)# interface Serial1                   (进入广域网口 1 子配置模式)
R3(config- if)# ip address 192.168.11.1 255.255.255.0 (配置 IP 地址)
R3(config- if)# bankwidth 64                    (设置带宽)
R3(config- if)# clockrate 64000                 (设置时钟频率)
R3(config)# exit

R3(config)# router igrp 100                 (进入 IGRP 协议配置子模式)
R3(config-router)# network 192.168.12.0 (说明路由器 R3 与 192.168.12.0 邻接)
R1(config-router)# network 192.168.11.0 (说明路由器 R3 与 192.168.11.0 邻接)
R1(config-router)# network 192.168.3.0  (说明路由器 R3 与 192.168.3.0 邻接)
```

11.3.6　EIGRP 协议配置

EIGRP 是增强型的 IGRP 协议，是典型的平衡混合路由选择协议，融合了距离矢量和链路状态两种路由选择协议的优点，使用一种散射更新算法，实现了更高的路由性能。运行 EIGRP 的路由器之间形成邻居关系，并交换路由信息，通过 Hello 包维持邻居关系。它将存储所有与其相邻路由器的路由表信息，以快速适应路由变化。EIGRP 路由器内包括一个相邻路由器表、一个拓扑结构表、一个路由表。它支持 VLSM、自动路由汇总，支持多种网络层协议。

1．EIGRP 路由配置常用命令

EIGRP 路由配置的常用命令如表 11-7 所示。

表 11-7　EIGRP 路由配置的常用命令

命　令	说　明
router eigrp autonomous-system	指定使用 EIGRP 协议，其中 autonomous-system 是自治系统号，EIGRP 协议只在相同自治系统号的路由器之间完成路由更新
network network-addr 掩码反码	指定与该路由器直接相连的网络。如果指定的网络是 A、B、C 类，则无须加入掩码反码；如果是子网，则需要加入掩码反码
no auto-summary	关闭自动汇总功能

2．EIGRP 配置实例

EIGRP 配置拓扑图如图 11-6 所示。

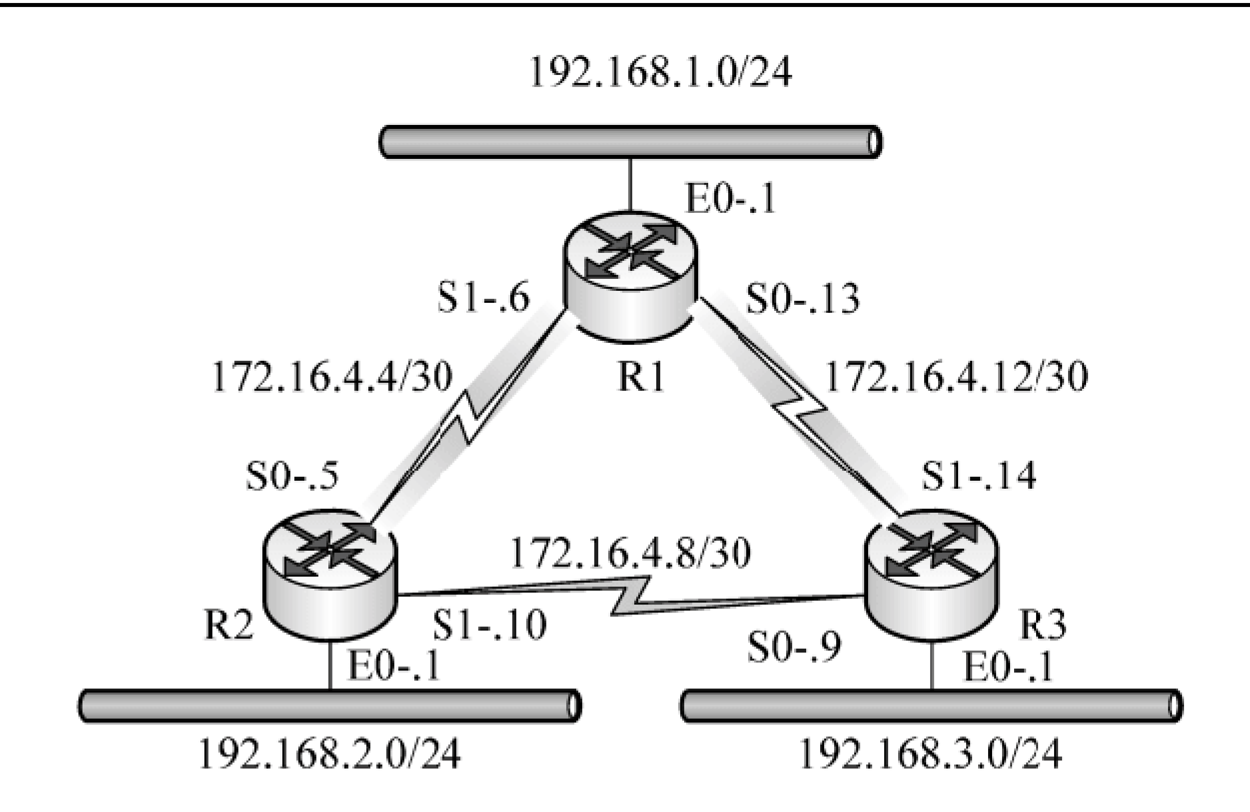


图 11-6　EIGRP 配置拓扑图

下面就以路由器 R1 为例，说明整个配置过程：

```
R1# config terminal                          (进入全局配置模式)
R1(config)# interface Ethernet0              (进入以太网口 0 子配置模式)
R1(config-if)# ip address 192.168.1.1 255.255.255.0 (配置 IP 地址)
R1(config)# exit
R1(config)# interface Serial0                (进入广域网口 0 子配置模式)
R1(config-if))# ip address 172.16.4.13 255.255.255.252 (配置 IP 地址)
R1(config-if))# bankwidth 1544               (设置带宽)
R1(config-if))# exit
R1(config)# interface Serial1                (进入广域网口 1 子配置模式)
R1(config-if))# ip address 172.16.4.6 255.255.255.252 (配置 IP 地址)
R1(config-if))# bankwidth 1544               (设置带宽)
R1(config-if))# clockrate 130000             (设置时钟频率)
R1(config-if))# exit

R1(config)# router eigrp 10                  (进入 IGRP 协议配置子模式)
R1(config-router)# network 172.16.4.4  0.0.0.3
R1(config-router)# network 172.16.4.12  0.0.0.3
R1(config-router)# network 192.168.1.0
```

注：在上面的配置中，network 172.16.4.4 和 172.16.4.12 是两个子网，因此需写出“掩码”的反码。

11.3.7　OSPF 协议配置

开放最短路径优先（OSPF）协议，和其他 SPF 一样，它采用的也是 Dijkstra 算法。OSPF 协议现在已成为最重要的路由选择协议之一，主要用于同一个自治系统。

OSPF 协议采用了“区域-area”的设计，提高了网络可扩展性，并且加快了网络汇

聚时间。也就是将网络划分成许多较小的区域，每个区域定义一个独立的区域号并将此信息配置给网络中的每个路由器。从理论上说，通常不应该采用实际地域来划分区域，而是应该本着使不同区域间的通信量最小的原则进行合理分配。

1．OSPF 路由配置常用命令

OSPF 路由配置的常用命令如表 11-8 所示。

表 11-8　OSPF 路由配置的常用命令

命　令	说　明
router ospf process-id	指定使用 OSPF 协议，其中 process-id 是其路由进程号，多个 OSPF 进程可以在同一个路由上配置，但通常不要这样做，该进程号只在路由器内部起作用，不同路由器可以不同
Network 网码地址 掩码反码 area 区域号	指定与该路由器直接相连的网络。掩码反码可以用 255.255.255.255 减去掩码得到。区域号可以是数字，也可以是 IP 地址。ID 为 0 表示是主干域，不同网络区域的路由器通过主干域学习路由
area 区域号 stub	将某区域转换成根区（不繁殖外部路由的区域）
show ip ospf neighbor	列出与本路由器是“邻居”关系（也就是进行路由信息交换的）的路由器
no ospf auto-cost-determination	OSPF 会自动根据每个接口的带宽，计算出其 cost（代价）：cost=10^8÷带宽(单位为 bps)。如果要手动配置，则可使用该命令使其不自动计算
ip ospf cost	手动设置接口 cost

2．OSPF 配置实例

下面以图 11-7 所示的一个网络为例来说明 OSPF 路由选择协议的配置方法，该网络中有 0 和 1 两个区域，其中 R1 的 S1 端口、R2 的 S0 端口属于区域 0；而 R3、R1 的 S0 端口、R2 的 S1 端口则属于区域 1。

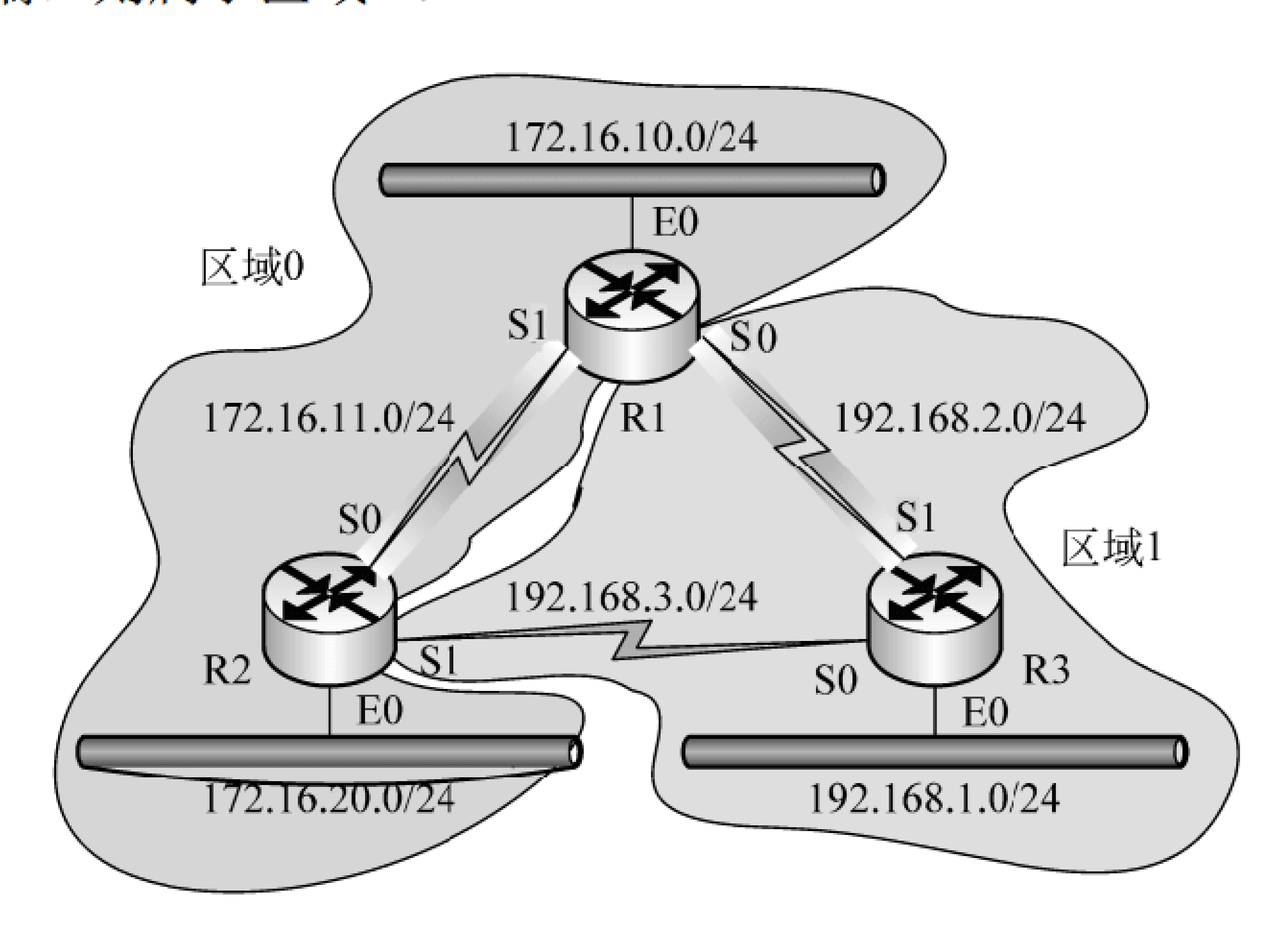


图 11-7　OSPF 配置拓扑图

下面列出三个路由器配置 OSPF 的指令。

```
R1# config terminal                          (进入全局配置模式)
R1(config)# router ospf 100                  (进入 OSPF 协议配置子模式)
R1(config-router)# network 172.16.10.1  0.0.0.0  area 0   (设置邻接网络)
R1(config-router)# network 172.16.11.1  0.0.0.0  area 0   (指定区域 0)
R1(config-router)# network 192.168.2.1  0.0.0.0  area 1

R2(config)# router ospf 200                  (进入 OSPF 协议配置子模式)
R2(config-router)# network 172.16.0.0  0.0.255.255  area 0 (设置邻接网络)
R2(config-router)# network 192.168.3.0  0.0.0.255  area 1

R3(config)# router ospf 300                  (进入 OSPF 协议配置子模式)
R3(config-router)# network 192.0.0.0  0.255.255.255  area 1 (设置邻接网络)
```

从上面的配置实例中可知，在配置 OSPF 时可以将子网进行合并，以减少条目，提高效率。例如 R3，其邻接子网是 192.168.1.0、192.168.2.0、192.168.3.0 三个，因此可以合并为 192.0.0.0/255.0.0.0；当然合并为 192.168.0.0/255.255.0.0 也是可行的。

11.3.8 访问控制列表 ACL 配置

访问控制列表通过限制使用者或设备来达到控制网络流量、解决网络拥塞、提高安全性等目的。在 IP 网络中，可以使用的访问列表有标准访问列表（值为 1～99）、扩展访问列表（标号为 100～199）两种。

1．标准访问列表

功能说明：基于源 IP 地址来进行判定是否允许或拒绝数据报通过（或其他操作，例如在 NAT 中判断是否进行地址转换）。

命令格式：

```
access-list access-list-number {permit | deny}
{source [ source-wildcard] | any }
```

命令解释：

- access-list：访问列表命令。
- access-list-number：访问列表号码，值为 1～99。
- permit：允许。
- deny：拒绝。
- source：源 IP 地址。
- source-wildcard：源 IP 地址的通配符。

- any：任何地址，代表 0.0.0.0 255.255.255.255。
- 通配符：source-wildcard 省略时，则使用默认值 0.0.0.0。它的作用与子网掩码是不相同的，当其取值为 1 时，代表该位不必强制匹配；当其取值为 0 时，代表必须匹配。

因此，如果 source 是 203.66.47.0，source-wildcard 是 0.0.0.255，则说明只要前三组符合，最后一组可以不符合，即有一个 C 类的 IP 地址符合。

这个命令的实例如下：

```
access-list 1 permit 202. 1. 2.3        （允许 IP 地址为 202.1.2.3 的数据包通过）
access-list 2 permit 202. 1. 2.3 0.0.0.255 （允许网络 202.1.2.0 的数据包通过）
access-list 3 deny 202. 1. 2.3          （禁止 IP 地址为 202.1.2.3 的数据包通过）
access-list 5 deny 202. 1. 2.3
access-list 5 permit any
（禁止 IP 地址为 202.1.2.3 的数据包通过，但允许其他任何 IP 的数据包通过）
```

2．扩展访问列表

功能说明：在标准访问列表的基础上增加更高层次的控制，它能够基于目的地址、端口号码、对话层协议来控制数据报。

命令格式：

```
access-list access-list-number { permit | deny }
{protocol \ protocol-keyword }
{source [ source-wildcard ] | any }
{destination destination-wildcard ] | any }
            [ protocol-specific options] [ log ]
```

命令解释：

- protocol \ protocol-keyword：可使用的协议，包括 IP、ICMP、IGRP、EIGRP、OSPF 等。
- destination destination-wild：目的 IP 地址，格式与源 IP 地址相同。
- protocol-specific options：协议指定的选项。
- log：记录有关数据包进入访问列表的信息。

这个命令的实例如下：

```
access-list 100 deny ip any 11.0.0.0 0.255.255.255
access-list 100 permit ip any any
（禁止任何 IP 地址访问 11.0.0.0/8 网络的 IP 数据报，允许其他的访问）
access-list 150 permit tcp any host 10.64.0.2 eq smtp
（允许以 SMTP 协议访问 10.64.0.2）
```

11.3.9 网络地址转换配置

网络地址转换（NAT）的应用场景主要有两种：一是从安全角度考虑，不想让外部网络用户了解自己的网络结构和内部网络地址；二是从 IP 地址资源角度考虑，当内部网络人数太多时，可以通过 NAT 实现多台设备共用一个合法 IP 访问 Internet。

NAT 设置可以分为静态地址转换、动态地址转换、复用动态地址转换三种。

1．静态地址转换

静态地址转换将本地地址与合法地址进行一对一的转换，且需要指定其与哪个合法地址进行转换。如果内部网络有 E-mail 服务器或 FTP 服务器等可以为外部用户提供的服务，这些服务器的 IP 地址必须采用静态地址转换，以便外部用户可以使用这些服务。整个配置过程包括三个步骤，如表 11-9 所示。

表 11-9 静态路由配置

步 骤	功 能	命 令
1	在内部地址和合法地址之间建立静态转换	ip nat inside source static 内部地址 合法地址
2	指定连接网络的内部端口	ip nat inside
3	指定连接外部网络的外部端口	ip nat outside

如图 11-8 所示的是一个静态 IP 地址转换的例子。

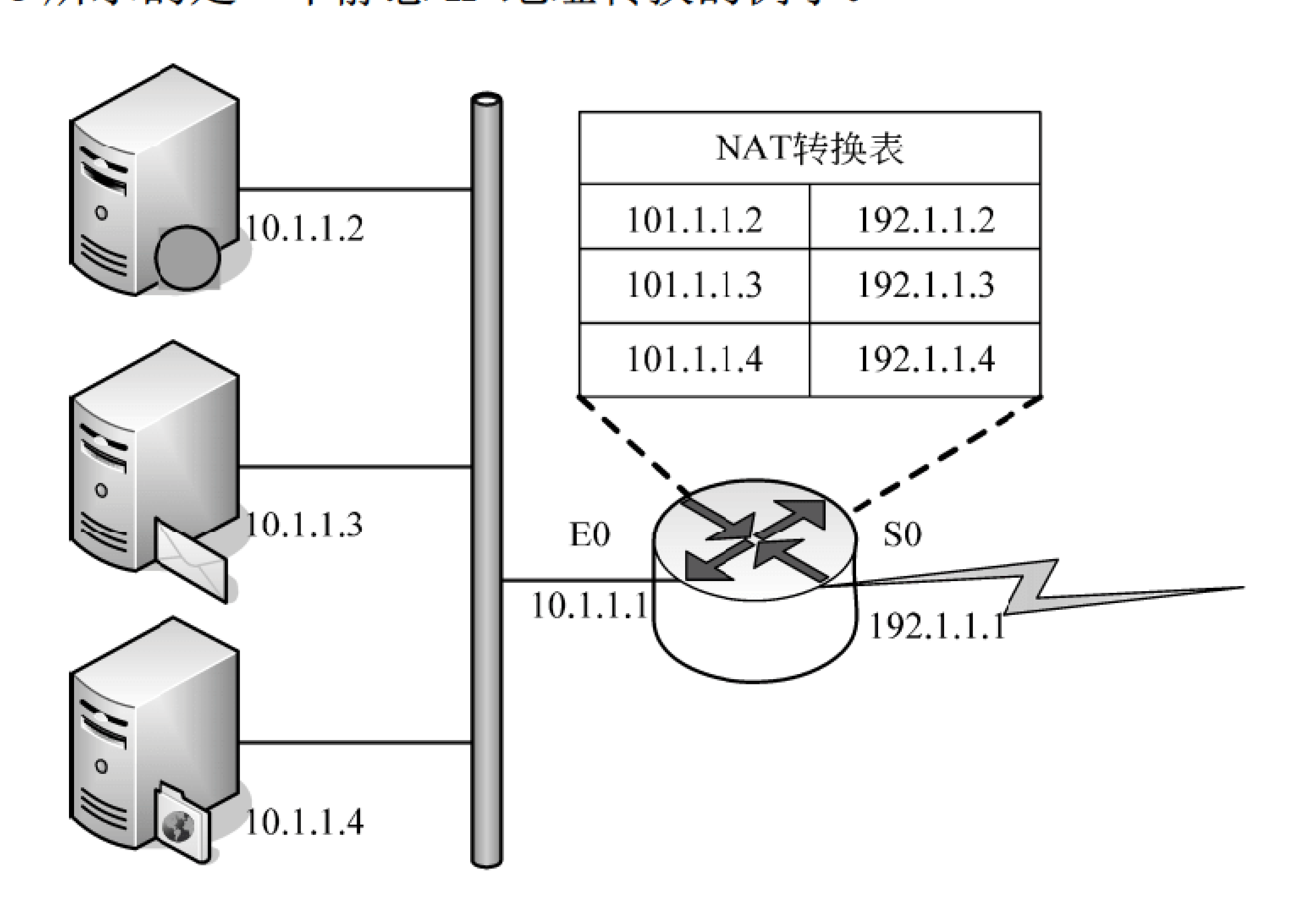


图 11-8 静态 IP 地址转换示例

```
ip nat inside source static 10.1.1.2 192.1.1.2
ip nat inside source static 10.1.1.3 192.1.1.3
ip nat inside source static 10.1.1.4 192.1.1.4
```

（手动设置静态的映射关系）

```
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
ip nat inside        （说明该端口是内网接口）

interface Serial0
ip address 192.1.1.1 255.255.255.0
ip nat outside       （说明该端口是外网接口）
```

2．动态地址转换

动态地址转换也是将本地地址与合法地址进行一对一的转换，但是动态地址转换是从合法地址池中动态地选择一个未使用的地址与本地地址进行转换。其配置包括 5 个步骤，如表 11-10 所示。

表 11-10　动态地址转换配置

步　　骤	功　　能	命　　令
1	定义合法地址池	ip nat pool 地址池名称 起始 IP 地址 终止 IP 地址 子网掩码
2	定义一个标准的访问列表规则，指出允许哪些内部地址可进行动态地址转换	access-list 标号 permit 源地址 通配符 其中标号为 1～99 间的整数
3	将由访问列表指定内部地址与指定的合法地址池进行地址转换	ip nat inside source list 访问列表标号 pool 地址池名称
4	指定与内部网络相连的内部端口	ip nat inside
5	指定连接外部网络的外部端口	ip nat outside

对于如图 11-8 所示的例子，采用动态地址映射的配置如下所示：

```
ip nat pool PoolA 192.1.1.2 192.1.1.10 netmask 255.255.255.0
（设置合法地址池，名为 PoolA，地址范围是 192.1.1.2~192.1.1.10）
ip nat inside source list 1 pool PoolA
（对访问列表 1 中设置的本地地址，应用 PoolA 池进行动态地址转换）

interface Ethernet0
ip address 10.1.1.1 255.255.255.0
ip nat inside        （说明该端口是内网接口）

interface Serial0
ip address 192.1.1.1 255.255.255.0
ip nat outside       （说明该端口是外网接口）

access-list 1 permit 10.1.1.0 0.0.0.255（10.1.1.0/24 的本地地址进行 NAT 转换）
```

3．复用动态地址转换

复用动态地址转换首先是一种动态地址转换，但是它可以允许多个本地地址共用一个合法地址。对于只申请到少量 IP 地址，但却经常同时有多于合法地址个数的用户上外部网络的情况，这种转换极为有用。复用地址转换的配置如表 11-11 所示。

表 11-11　复用地址转换配置

步　骤	功　能	命　令
1	定义合法地址池	ip nat pool 地址池名称 起始IP地址 终止IP 地址 子网掩码
2	定义一个标准的访问列表规则，指出允许哪些内部地址可进行动态地址转换	access-list 标号 permit 源地址 通配符 其中标号为 1～99 间的整数
3	在本地地址和合法 IP 地址间建立复用动态地址转换（与动态地址转换相比，就是加上 overload）	ip nat inside source list 访问列表标号 pool 地址池名称 overload
4	指定与内部网络相连的内部端口	ip nat inside
5	指定连接外部网络的外部端口	ip nat outside

假设在如图 11-8 所示的网络中，只有两个外部地址：192.1.1.1 和 192.1.1.2，显然不够用，因此就必须采用复用动态地址转换法。相比上一个而言，修改的只有其中的两句：

```
ip nat pool PoolA 192.1.1.1 192.1.1.2 netmask 255.255.255.0
（设置合法地址池，名为 PoolA，地址范围是 192.1.1.1~192.1.1.2）
ip nat inside source list 1 pool PoolA overload
（对访问列表 1 中设置的本地地址，应用 PoolA 池进行复用动态地址转换）
```

11.4　例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 12 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

路由器中加入一条主机路由，地址为 200.115.240.0，子网掩码是__（1）__。

（1）A．255.255.0.0　　B．255.255.240.0

C．255.255.255.0　　D．255.255.255.255

例题 1 分析

本题考查的是主机路由的概念。路由表中一般使用的是目的主机所在的网络而不是单个主机，但作为特性，IP 也允许指定某个目的主机的路由，称为指定主机路由，子网掩码采用 255.255.255.255，这是对 IP 地址的全匹配。

例题 1 答案

（1）D

例题 2

通过路由器的访问控制列表（ACL）可以__（2）__。

（2）A．进行域名解析　　B．提高网络的利用率

C．检测网络病毒　　D．进行路由过滤

例题 2 分析

访问控制列表（ACL）是应用在路由器接口的指令列表。这些指令列表用来告诉路由器哪些数据包可以收、哪些数据包需要拒绝。至于数据包是被接收还是被拒绝，可以由类似于源地址、目的地址、端口号等特定指示条件来决定。

例题 2 答案

（2）D

例题 3

通过 Web 管理交换机，在 URL 栏中输入__（3）__。

（3）A．交换机的用户名　　B．交换机的 MAC 地址

C．IP 地址　　D．端口号

例题 3 分析

交换机可以通过 Web（网络浏览器）来管理，但是必须给交换机指定一个 IP 地址。在默认状态下，交换机没有 IP 地址，必须通过串口或其他方式指定一个 IP 地址之后，才能启用这种管理方式。

例题 3 答案

（3）C

例题 4

仿真终端与交换机控制台端口（Console）__（4）__。

（4）A．通过因特网连接　　B．用 RS-232 电缆连接

C．用电话线　　D．通过局域网连接

例题 4 分析

交换机都带有一个控制端口“Console”，用来与计算机或终端设备进行连接，通过特定的软件来进行交换机的配置。所有交换机都安装了控制台端口，使用户或管理员能够利用终端与路由器进行通信，完成交换机配置。该端口提供了一个 EIA/TIA-232 异步串行接口，用于在本地对交换机进行配置（首次配置必须通过控制台端口进行）。

Console 端口使用配置专用连线（RS-232）直接连接至计算机串口，利用终端仿真程序（如 Windows 下的“超级终端”）进行交换机本地配置。

例题 4 答案

（4）B

例题 5

路由器 Console 端口默认的数据速率为__（5）__。

（5）A．2400bps B．4800bps C．9600bps D．10Mbps

例题 5 分析

路由器 Console 口，主要连接终端或运行终端仿真程序的计算机，在本地配置路由器。它提供的默认速率为 9600bps。

使用 Console 端口连接的方式，通常也是使用“超级终端”仿真软件，具体配置参数如下：端口速率为 9600bps，数据位为 8，奇偶校验无，停止位为 1，流控无。

例题 5 答案

（5）C

例题 6

路由器命令“Router(config)# access-list 1 permit 192.168.1.1”的含义是__（6）__。

（6）A．不允许源地址为 192.168.1.1 的分组通过，如果分组不匹配，则结束

B．允许源地址为 192.168.1.1 的分组通过，如果分组不匹配，则检查下一条语句

C．不允许目标地址为 192.168.1.1 的分组通过，如果分组不匹配，则结束

D．允许目标地址为 192.168.1.1 的分组通过，如果分组不匹配，则检查下一条语句

例题 6 分析

本题考查路由器标准访问控制列表的配置格式及其表示的含义。具体参考本章访问控制列表配置内容。

例题 6 答案

（6）B

例题 7

在生成树协议（STP）中，根交换机是根据__（7）__来选择的。

（7）A．最小的 MAC 地址 B．最大的 MAC 地址

C．最小的交换机 ID D．最大的交换机 ID

例题 7 分析

STP 要求每个网桥分配一个唯一的标识（BID），BID 通常由优先级（2bytes）和网桥 MAC 地址（6bytes）构成。根据 IEEE 802.1d 规定，优先级值为 0～65 535，默认的优先级为 32 768（0x8000）。当交换机最初启动时，它假定自己就是根交换机，并发送次优的 BPDU，当交换机接收到一个更低的 BID 时，它会把自己正在发送的BPDU 的根 BID 替换为这个最低的根 BID，所有的网桥都会接收到这些 BPDU，并且判定具有最小 BID 值的网桥作为根网桥。

根据选举规则，选择较小的优先级的交换机，当优先级相同的时候，查找最小的

MAC 地址成为根交换机。

例题 7 答案

（7）C

例题 8

下面关于 802.1q 协议的说明中正确的是__（8）__。

（8）A．这个协议在原来的以太帧中增加了 4 个字节的帧标记字段

B．这个协议是 IETF 制定的

C．这个协议在以太帧的头部增加了 26 字节的帧标记字段

D．这个协议在帧尾部附加了 4 字节的 CRC 校验码

例题 8 分析

802.1q 协议由 IEEE 制定，根据 802.1q 封装协议，在发送数据包时，都在原来的以太网帧头中的源地址后增加了一个 4 字节的 802.1Q 标签，之后接原来以太网的长度或类型域，关于以太网桢头的封装格式，这 4 个字节的 802.1Q 标签头包含了 2 个字节的标签协议标识（TPID，它的值是 8100），和两个字节的标签控制信息（TCI），TPID 是 IEEE 定义的新的类型，表明这是一个加了 802.1Q 标签的本文。

例题 8 答案

（8）A

例题 9

新交换机出厂时的默认配置是__（9）__。

（9）A．预配置为 VLAN 1，VTP 模式为服务器

B．预配置为 VLAN 1，VTP 模式为客户机

C．预配置为 VLAN 0，VTP 模式为服务器

D．预配置为 VLAN 0，VTP 模式为客户机

例题 9 分析

Cisco 的交换机都有一个默认的 VLAN，即 VLAN1，默认工作模式就是服务器模式。

例题 9 答案

（9）A

例题 10

当启用 VTP 修剪功能后，如果交换端口中加入一个新的 VLAN，则立即__（10）__。

（10）A．剪断与周边交换机的连接

B．把新的 VLAN 中的数据发送给周边交换机

C．向周边交换机发送 VTP 连接报文

D．要求周边交换机建立同样的 VLAN

例题 10 分析

VTP 修剪是 VTP 协议的一个功能，它能减少中继链路上不必要的信息量。在缺少 VTP 修剪的情况下，发给某个 VLAN 的广播会送到每一个在中继上承载该 VLAN 的交换机。即使交换机上没有位于那个 VLAN 的端口也是如此。VTP 通过修剪，来减少不必要扩散的通信量，提高中继的带宽利用率。仅当中继链路接收端上的交换机在那个 VLAN 中有端口时，才会将该 VLAN 的广播和未知单播转发到该中继链路上。（VTP 修剪不会改变一条链路的生成树协议的特点），因此选项 A，B，D 的描述都是错误的。

启用 VTP 修剪的命令为：

```
C2950#vlan database
C2950(vlan)#vtp pruning
```

例题 10 答案

（10）C

例题 11

路由器命令 R1(config) # ip routing 的作用是__（11）__。

（11）A．显示路由信息　　B．配置默认路由
C．激活路由器端口　　D．启动路由配置

例题 11 分析

路由器命令 R1(config) # ip routing 的作用是启动路由配置，一般默认为启用。关闭后，路由器成为透明网桥。

例题 11 答案

（11）D

例题 12

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】

某单位有 1 个总部和 6 个分部，各个部门都有自己的局域网。该单位申请了 6 个 C 类 IP 地址 202.115.10.0/24～202.115.15.0/24，其中总部与分部 4 共用一个 C 类地址。现计划将这些部门用路由器互联，网络拓扑结构如图 11-9 所示。

【问题 1】

该网络采用 R1～R7 共 7 台路由器，采用动态路由协议 OSPF。由网络拓扑图可见，该网络共划分了三个 OSPF 区域，其主干区域为__（1）__，主干区域中，__（2）__为区域边界路由器，__（3）__为区域内路由器。

【问题 2】

下表是该系统中路由器的 IP 地址分配表。

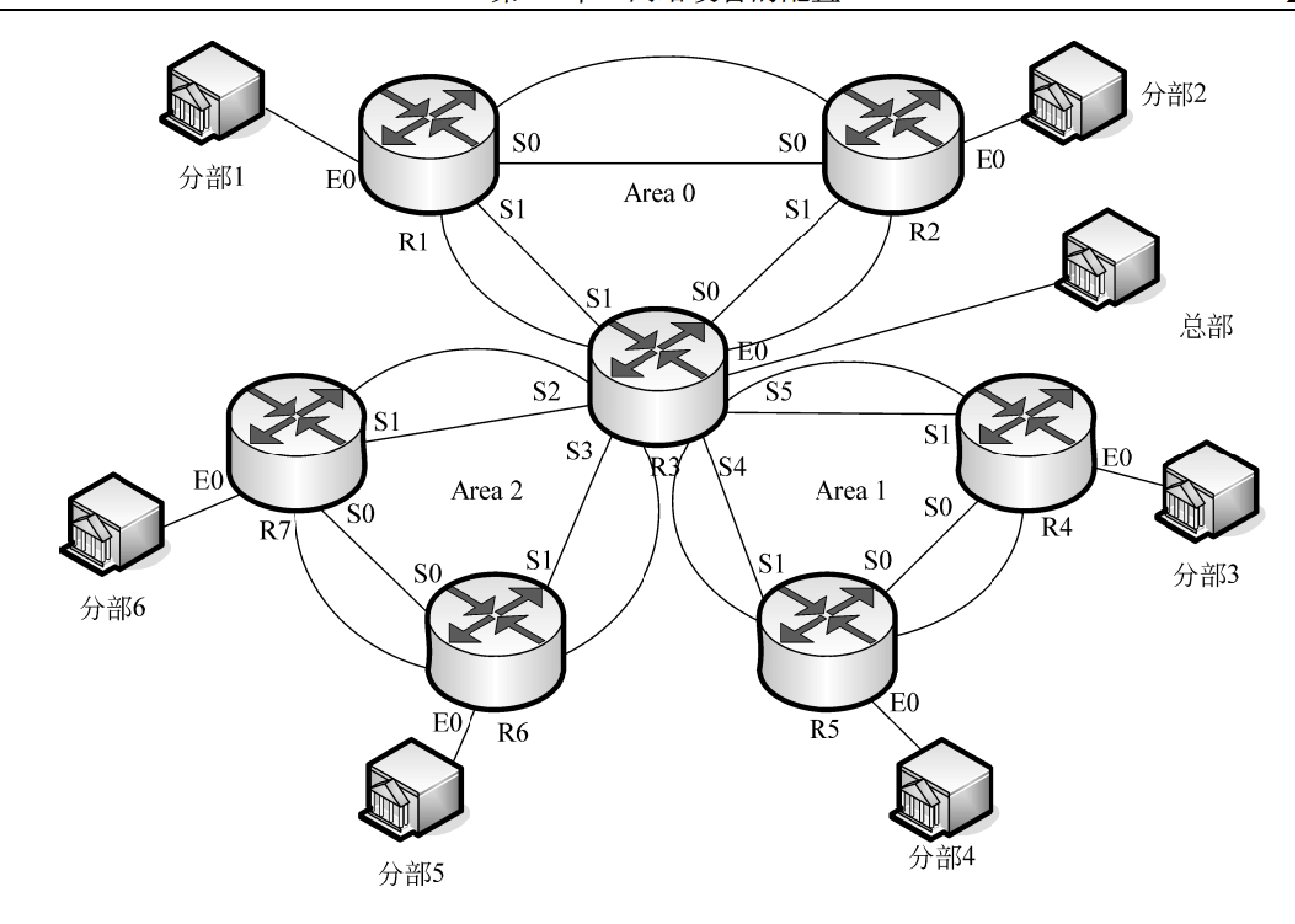


图 11-9　某单位网络拓扑图

路由器	端口 IP 地址	路由器	端口 IP 地址	路由器	端口 IP 地址
R1	E0:202.115.10.1/24	R4	E0:202.115.14.1/24	R6	E0:202.115.14.1/24
	S0:10.0.0.1/24		S0:10.0.3.2/24		S0:10.0.6.1/24
	S1:10.0.1.1/24		S1:10.0.5.1/24		S1:10.0.7.1/24
R2	E0:202.115.11.1/24	R5	E0:202.115.13.1/25	R7	E0:202.115.15.1/24
	S0:10.0.0.2/24		S0:10.0.3.1/24		S0:10.0.6.2/24
	S1:10.0.2.1/24		S1:10.0.4.1/24		S1:10.0.8.1/24

请根据网络拓扑图完成以下 R3 路由器的配置：

```
R3 (config)#interface e0/1                        (进入接口 e0/1 配置模式)
R3 (config-if)#ip address 202.115.13.254 __(4)__  (设置 IP 地址和掩码)
R3(config) # interface s0/0                       (进入串口配置模式)
R3(config-if) #ip address __(5)__ 255.255.255.0   (设置 IP 地址和掩码)
R3(config) # interface s0/1
R3(config-if) #ip address __(6)__ 255.255.255.0
R3(config) # interface s0/2
R3(config-if) #ip address __(7)__ 255.255.255.0
R3(config) # interface s0/3
R3(config-if) #ip address __(8)__ 255.255.255.0
```

```
R3(config) # interface s0/4
R3(config-if) #ip address  (9)   255.255.255.0
R3(config) # interface s0/5
R3(config-if) #ip address  (10)   255.255.255.0
```

【问题 3】

该单位部门 4 共有 110 台 PC，通过交换机连接路由器 R5 接入网络。其中一台 PC 的 IP 地址为 202.115.13.5，则其子网掩码应为 (11) ，网关地址应为 (12) 。

例题 12 分析

【问题 1】

OSPF 协议采用了“区域-area”的设计，提高了网络可扩展性，并且缩短了网络汇聚时间。也就是将网络划分成许多较小的区域，每个区域定义一个独立的区域号并将此信息转发给网络中的每个路由器。从理论上说，通常不应该采用实际地域来划分区域，而是应该本着使不同区域间的通信量最小的原则进行合理分配。OSPF 协议配置命令如下：

```
network 网码地址 掩码反码 area 区域号
```

该命令指定与该路由器直接相连的网络。掩码反码可以用 255.255.255.255 减去掩码得到。区域号可以是数字，也可以是 IP 地址。ID 为 0 表示是主干域，不同网络区域的路由器通过主干域学习路由。区域边界路由器（ABR）是位于一个或多个 OSPF 区域的一个路由器，其连接这个区域到骨干网络。ABR 被认为既是 OSPF 骨干区域也是内部区域的一部分，所以其既有骨干拓扑也有其他区域的拓扑路由表。在 Area 0 区域中，可以明显地区分出，区域边界路由器为 R3，区域内路由器为 R1、R2。

【问题 2】

本题考查的是为边界路由器 R3 端口配置 IP 地址即子网掩码。题中已指出，总部（使用 E0 端口与 R3 连接）与分部 4（使用 E0 端口与 R5 连接）是共用同一子网，因此它们两个使用的网段及掩码是完全相同的。根据表 1-1 中指示的 R5 的 E0 端口配置信息为：202.115.13.1/25，因此，R3 的 E0 端口掩码配置为 255.255.255.128。

第（5）空处，要求配置 R3 的 S0 的 IP 地址信息。已知 R3 的 S0 的对端是 R2 的 S1 端口，两者必须在同一网段，从表 1-1 中已知 R2 的 S1 端口 IP 为 10.0.2.1/24，因此，R3 的 S0 的 IP 地址配置范围只能从 10.0.2.2～10.0.2.254。第（6）～（10）空可按上述方法进行推算。

【问题 3】

前面提到过，分部 4 通过交换机接入，再通过 R5 的 E0 端口与路由器 R5 连接，从表 1-1 中可得知 R5 的 E0 端口 IP 为 202.115.13.1，子网掩码为 255.255.255.128，来作为该分部的网关。那么该分部 PC 的子网掩码应与其网关一致，为 255.255.255.128，网关地址即 E0（R5）地址为 202.115.13.1。

例题 12 答案

【问题 1】

（1）Area 0

（2）R3

（3）R1 和 R2

【问题 2】

（4）255.255.255.128

（5）10.0.2.2～10.0.2.254 之间任意一个地址

（6）10.0.1.2～10.0.1.254 之间任意一个地址

（7）10.0.8.2～10.0.8.254 之间任意一个地址

（8）10.0.7.2～10.0.7.254 之间任意一个地址

（9）10.0.4.2～10.0.4.254 之间任意一个地址

（10）10.0.5.2～10.0.5.254 之间任意一个地址

【问题 3】

（11）255.255.255.128

（12）202.115.13.1

第 12 章　网络服务器的配置

根据对考试大纲的分析以及历年的考试情况总结，本章出题数应在 5 分左右，约占上午考试的 7%。而在下午考试中，占有较大的比重，基本稳定在 30 分左右，至少也会考查 15 分。

本章中最常考查的知识点是 IP 地址、子网掩码的规划配置、Windows 系统下 DNS 服务器、DHCP 服务器、Web 服务器、FTP 服务器、E-mail 服务器、代理服务器等的配置。

希赛教育专家特别提示：虽然在考试大纲中对 Linux 平台下服务器配置未作明确规定，但 Linux 系统下 Samba 共享服务器、DHCP 服务器、DNS 服务器、FTP 服务器、邮件服务器配置等也是经常考查的内容。

12.1　IP 地址、子网掩码的规划配置

在规划设计网络 IP 地址时，一定要充分考虑网络的扩展性，一时的“节约”可能会导致日后大规模的地址变更，后者的工作量非常之大，且会带来一些不必要的麻烦。比如服务器地址变更会影响到访问，部分访问者可能对变更地址并不知晓(尤其是领导层)，过渡期可能非常长，会影响到正常业务的开展。当主机数目确定时，也要尽量避免地址分配“刚刚好”的思想。

由于 C 类网络可扩展性小，在规划设计大型网络时，通常使用 A 类或者 B 类网络地址，而配以 C 类网络掩码（如 255.255.255.0），这样的好处是给每一个局域网留出很大的地址空间，便于各个局域网的地址分配和扩展。这点在设计按照区域、部门划分的大型网络时尤为适用。比如使用 A 类地址 58.0.0.0，配以 255.255.255.0 网络掩码。

对于极小网络，比如网络掩码是 255.255.255.252 只有两个可用地址，通常适用于提供给拨号外接使用或者用于接入 ISP。比如某公司局域网为便于员工出差时能够随时访问公司内部网络，需要提供 PPP 拨号服务，当提供电话线路非常少时（仅一条），就可以使用这类超小网络以便于节约网络资源。当然在电话线路较多的时候，需要使用地址池。

路由器的地址一般选择当前网络中最大的 IP 地址，如以 C 类网络为例，网络地址为 195.142.133.0，网络掩码为 255.255.255.0，一般使用 195.142.133.254 作为路由器地址，195.142.133.253 作为局域网交换机地址，但是这并没有什么强制的规定。195.142.133.1～195.142.133.30 作为局域网内服务器或者受控保密计算机 IP 地址使用，这样便于防火墙

等网络设备的配置。

1．Linux 网络配置

手工配置网络可以使用命令/sbin/ifconfig 即可，不用另外编辑任何文件。手工改变网络配置时，需要注意的是很多网络服务正在运行，它们可能不会检查新的网络掩码和广播地址，所以在改变接口参数之前，要使用 down 选项使该接口暂时不能被使用。

一般手工配置网络参数的命令如下：

```
# /sbin/ifconfig  eth0  ipaddress  netmask  netmask  broadcast  broadcast
```

比如要修改 eth0 的子网掩码和广播地址，ifconfig 命令如下：

```
# /sbin/ifconfig  eth0 down
# /sbin/ifconfig  eth0  netmask  new_netmask  broadcast  new_broadcast  up
```

例如分配给某单位一个 B 类网络地址：158.103.201.0，子网掩码为 255.255.255.0，可以有 158.103.201.1～158.103.201.254 的 IP 地址。如果将其分配为 A 和 B 两个子网，则每个子网的子网掩码变成 255.255.255.128，子网地址分别为 A 子网：158.103.201.1～158.103.201.126，B 子网：158.103.201.129～158.103.201.254。每个子网上主机网络参数配置如下：

A 子网：

```
# /sbin/ifconfig eth0 ipaddress netmask 255.255.255.128 broadcast 158.103.
201.127
```

B 子网：

```
# /sbin/ifconfig eth0 ipaddress netmask 255.255.255.128 broadcast 158.103.
201.255
```

利用/sbin/ifconfig 命令可以显示所有网络参数：

/sbin/ifconfig　-a

2．Windows 2003 网络配置

在 Windows 2003 安装系统时，网卡就已经被安装，并配以最基本的网络协议，当然包括 TCP/IP。因此在 Windows 2003 下的网络配置主要是后期的更改。

单击屏幕左下角的“开始”按钮，然后依次选择“设置”→“网络和拨号连接”→“本地连接”命令，或者在桌面“网上邻居”上单击鼠标右键，选择“属性”→“本地连接”命令，或者双击屏幕右下角网络连接图标，然后进入如图 12-1 所示的界面。

单击“属性”按钮，如图 12-2 所示。

双击“Internet 协议（TCP/IP）”项，进入图 12-3 所示的界面。

这时就可以按照需要对 IP 地址、子网掩码和默认网关进行配置了。



图 12-1 本地连接状态

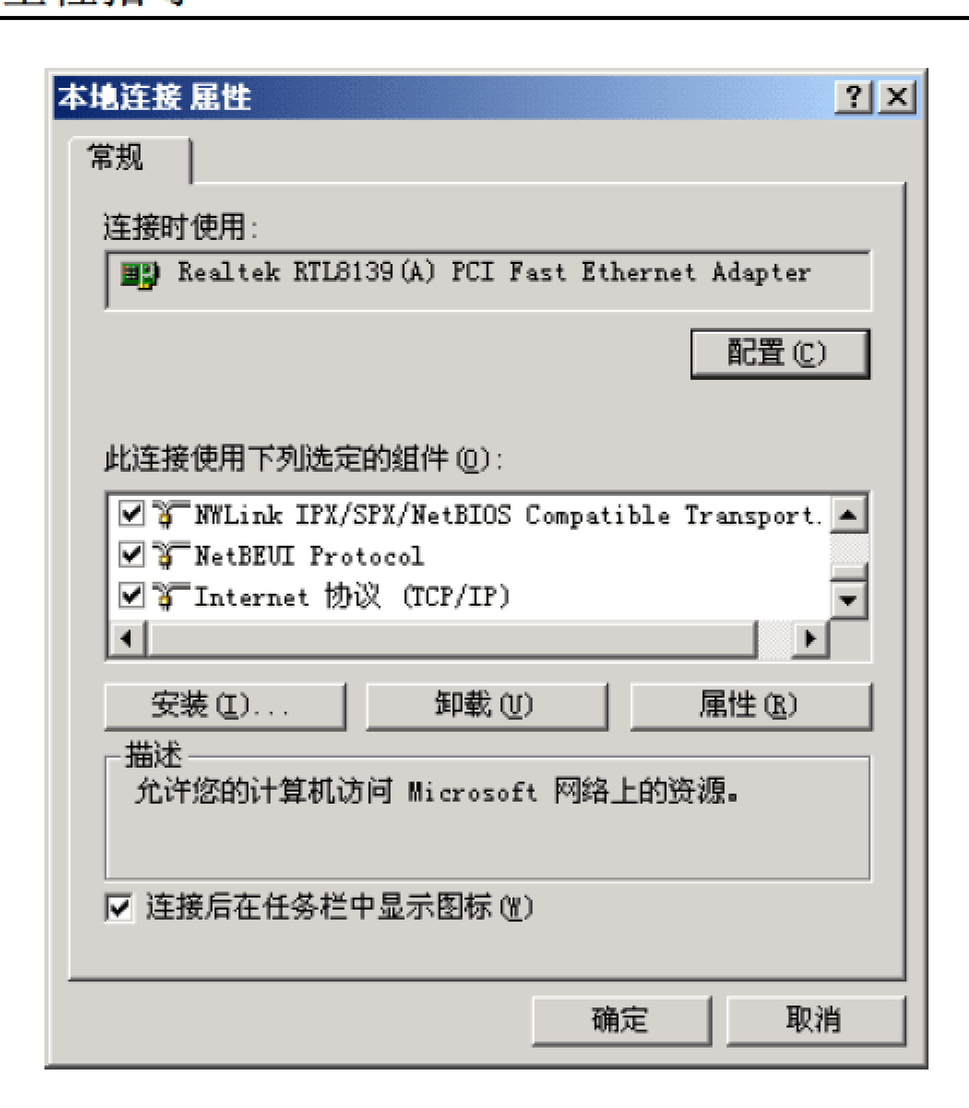


图 12-2 本地连接属性

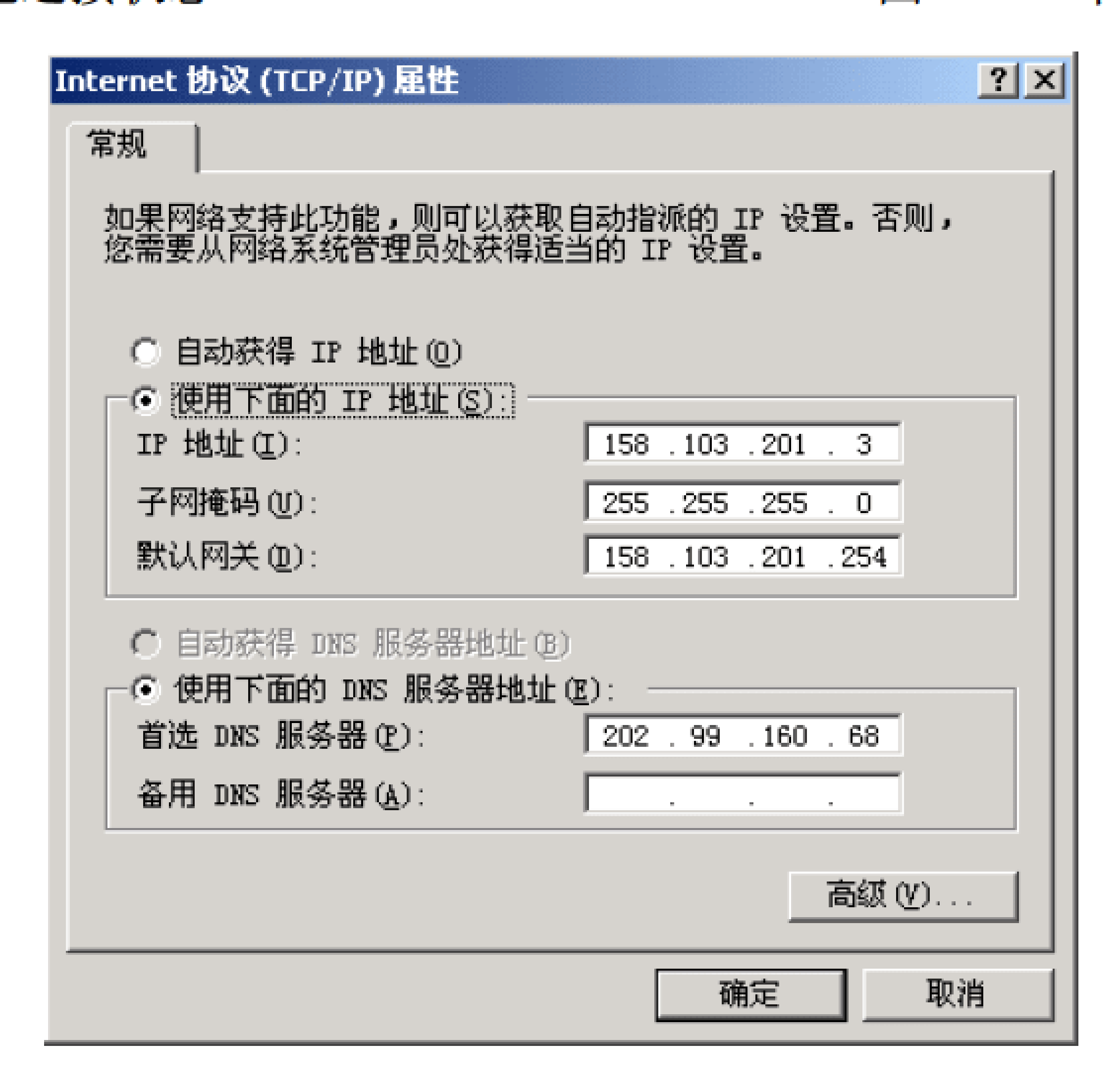


图 12-3 Internet 协议属性

12.2 IIS 服务配置

本知识点在于了解 IIS 组件及其提供服务的相关概念与配置，掌握 Web 服务器、FTP 服务器和 E-mail 服务器的配置方法，相关配置文件和参数。

IIS（Internet Information Server，因特网信息服务）是一种 Web（网页）服务组件，其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，它使得在网络（包括互联网和局域网）上发布信息成了一件很容易的事。

1）IIS 的安装

进入“控制面板”，依次选择“添加/删除程序→添加/删除 Windows 组件”，启动 Windows 组件向导，在“组件”列表中，选中“应用程序服务器”复选框，单击详细信息，如图 12-4 所示。



图 12-4　安装 IIS 服务（一）

在“Internet 信息服务（IIS）的子组件”中勾选想要添加的服务，比如 FTP、SMTP 等等，如图 12-5 所示。



图 12-5　安装 IIS 服务（二）

2）IIS 的运行

当 IIS 添加成功之后，再选择“开始”→“设置”→“控制面板”→“管理工具”→“Internet 服务管理器（Internet 信息服务）”以打开 IIS 管理器，对于有“已停止”字样的服务，均在其上单击鼠标右键，选择“启动”来开启。

12.2.1 用 IIS 架设 Web 服务器

本节主要介绍 IIS 下 Web 服务器的配置。

1. 站点主目录

安装 IIS 后，系统会自动创建一个默认 Web 站点和一个默认 FTP 站点供用户使用。其中，Web 站点与 FTP 站点的默认主目录分别是：%SYSTEMROOT%\Inetpub\wwwroot 和%SYSTEMROOT%\Inetpub\ftproot，其中 SYSTEMROOT 是操作系统根目录。

主目录确定后，用户只需要将要发布的内容复制到该目录下即可。主目录的设置步骤如下：

首先，选择“开始”→“程序”→“管理工具”→“Internet 服务管理器”命令，打开“Internet 信息服务管理器”窗口，如图 12-6 所示。

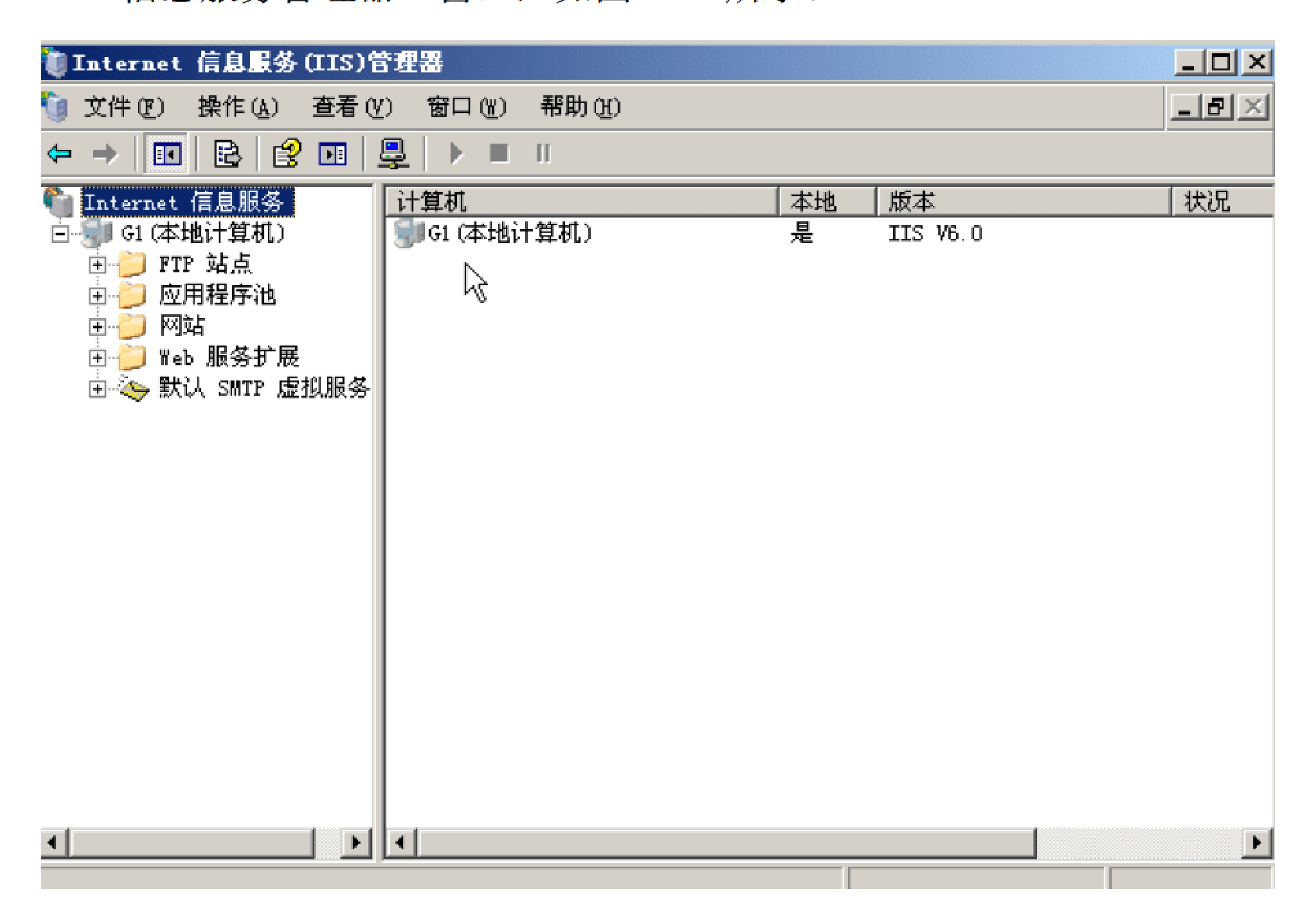


图 12-6 Internet 信息服务管理器

然后，在控制台目录树中，展开“网站”节点，右击鼠标“默认 Web 站点”节点，从弹出的快捷菜单中选择“属性”命令，打开“默认网站属性”对话框，并切换到“主目录”选项卡，如图 12-7 所示。

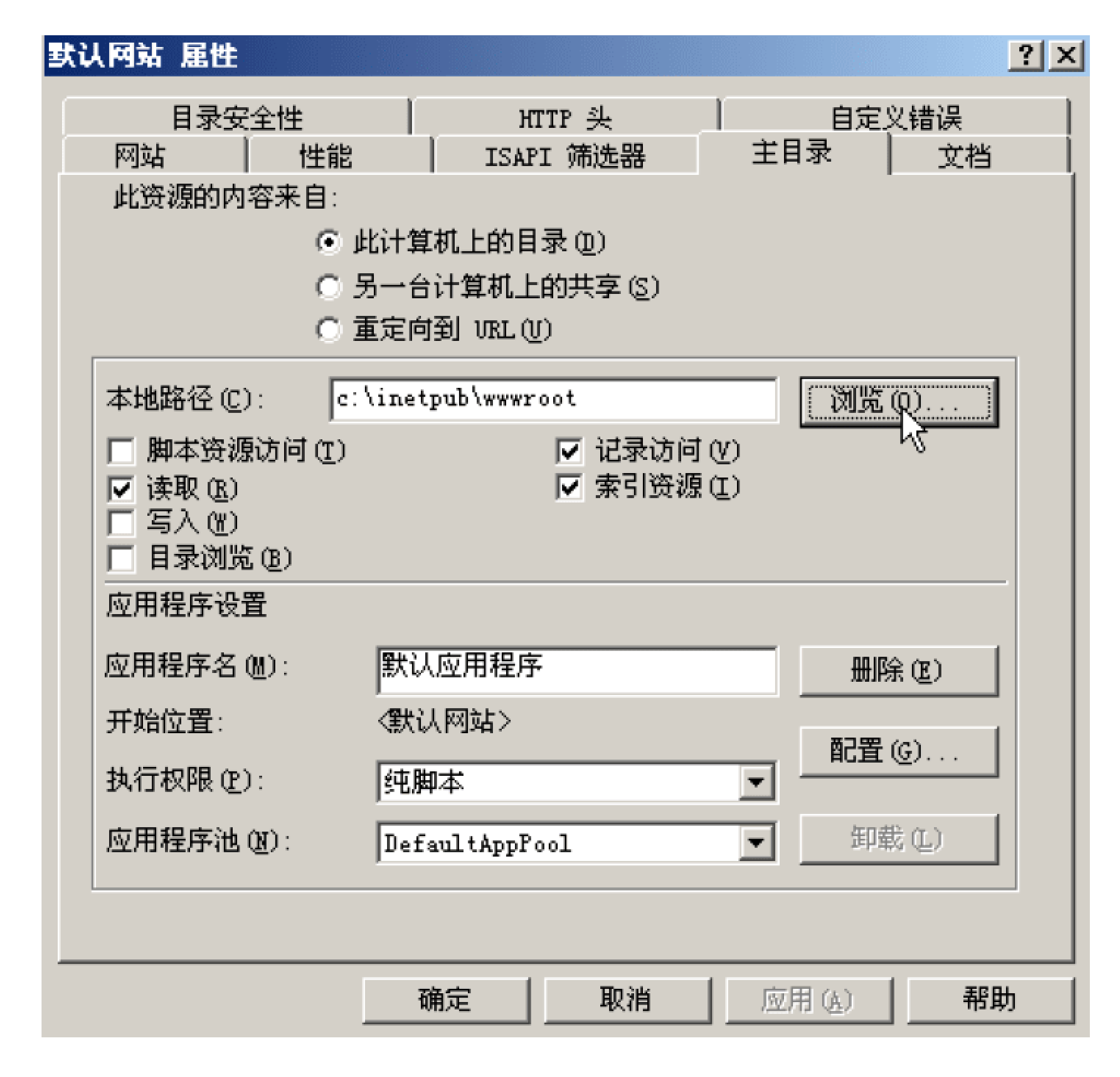


图 12-7　设置主目录

2．默认文档

默认文档是指在浏览器请求指定文档名的时候提供的文档，它可以是目录的主页，也可以是包含站点文档目录列表的索引页。启用默认文档的操作步骤如下：

首先，打开“Internet 信息服务”控制台窗口，在控制台目录树中、右击要添加页脚文件的 Web 站点或目录，从弹出的快捷菜单中选择“属性”命令，打开默认 Web 站点“属性”对话框，并切换到“文档”选项卡，如图 12-8 所示。

在图 12-8 中，选中“启用默认文档”复选框，则系统默认的文档为 Default.htm 和 Default.asp。如果管理员要添加默认文档，可单击“添加”按钮，打开“添加默认文档”对话框，输入文档名，确定后，系统将会按出现在列表中的文档名称的顺序提供默认文档，并返回所找到的第一个文档。

3．站点虚拟目录

要从主目录以外的其他目录中进行内容发布，就必须创建虚拟目录。“虚拟目录”不包含在主目录中，但显示给客户浏览器时却像位于主目录中一样。虚拟目录和实际目录都显示在 Internet 服务管理器中。虚拟目录由右下角带有地球的文件夹的图标来表示。对于简单的 Web 站点，不需要添加虚拟目录，而将所有文件放置在站点的主目录中。但是，如果站点比较复杂，或者需要为站点的不同部分指定不同的 URL 时，就需要创建虚拟目录。

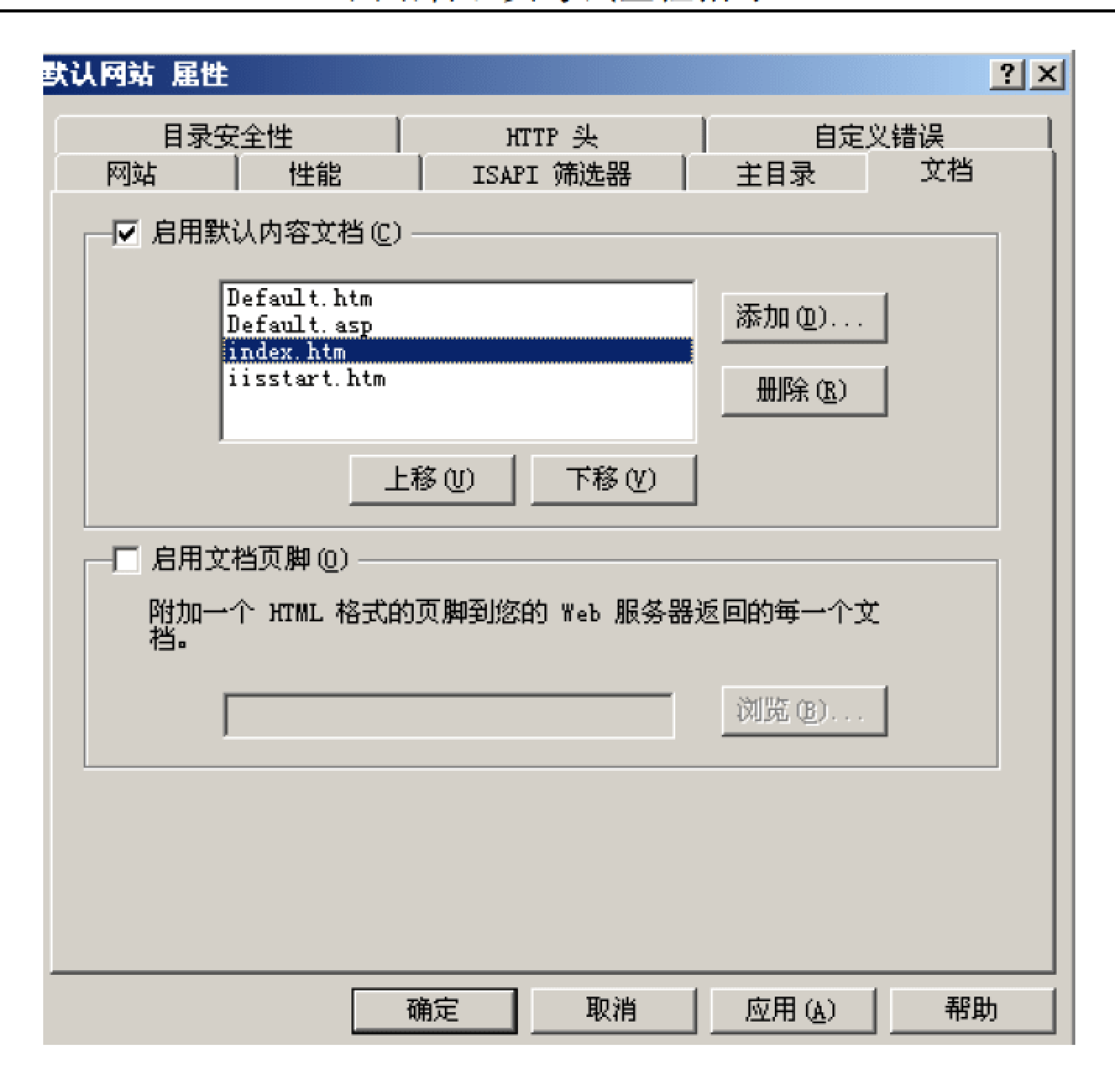


图 12-8 “文档”选项卡

创建虚拟目录的操作步骤如下：

首先，打开“Internet 信息服务”管理器，在控制台目录树中展开 server 节点。

然后，右击“默认 Web 站点”节点，从弹出的快捷菜单中选择“新建”→“虚拟目录”命令，打开“虚拟目录创建向导”对话框。单击“下一步”按钮，打开“虚拟目录别名”对话框，如图 12-9 所示。



图 12-9 虚拟目录别名对话框

在图 12-9 中，在“别名”框中输入用于获得此 Web 虚拟目录访问权限的别名。单击“下一步”按钮，打开“网站内容目录”对话框，如图 12-10 所示。输入虚拟目录的路径。



图 12-10　网站内容目录

在图 12-10 中，单击“下一步”按钮，打开“访问权限”对话框。在“允许下列权限”选项组中，为此目录设置访问权限，如图 12-11 所示。

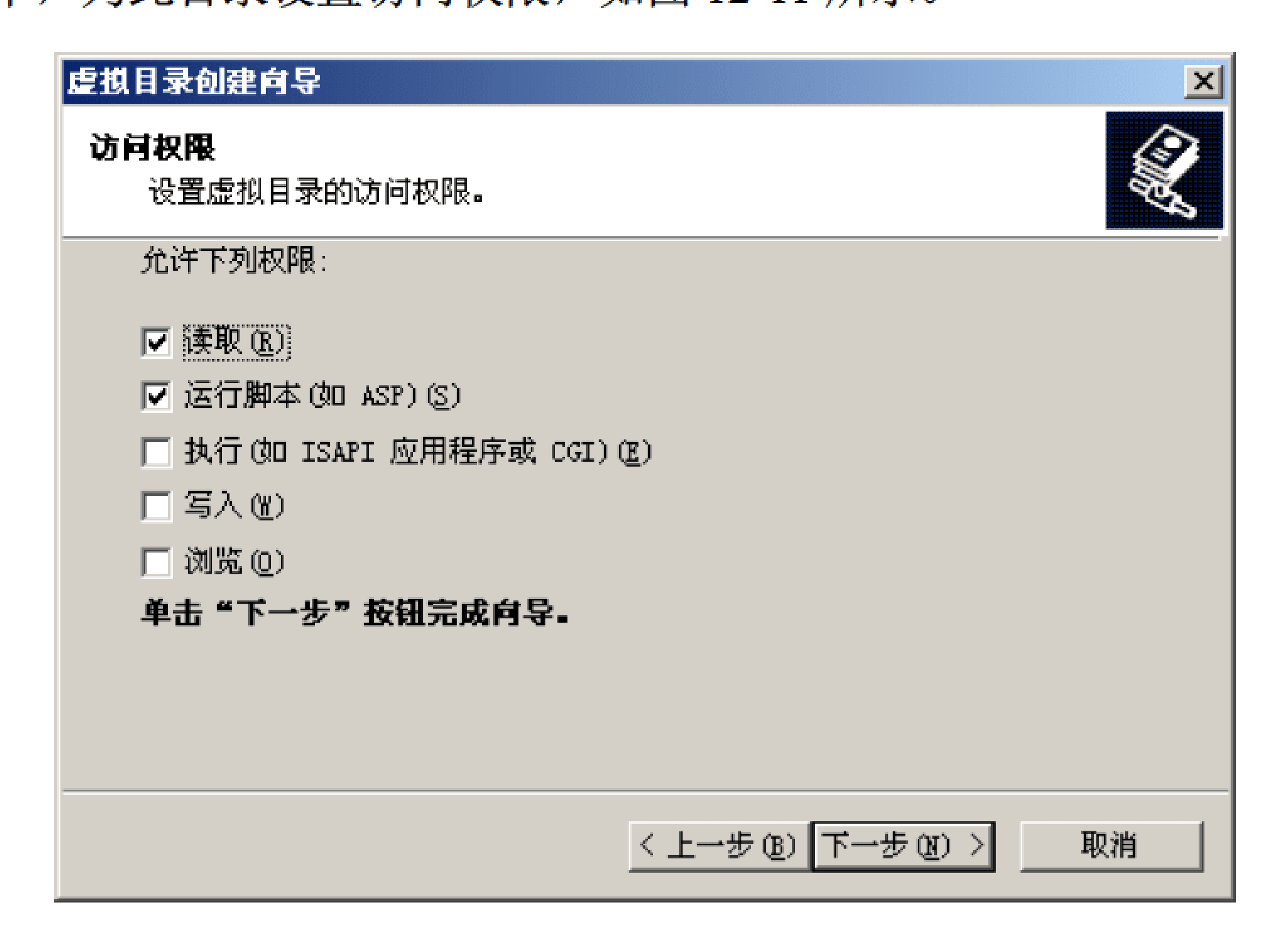


图 12-11　设置访问权限

在图 12-11 中，单击“下一步”按钮，打开“您已成功完成‘虚拟目录创建向导’”

对话框，完成虚拟目录的创建。

12.2.2 用 IIS 架设 FTP 服务器

同 Web 站点一样，每个 FTP 站点也必须有一个主目录，作为其他访问者访问用户 FTP 站点的起点。在 FTP 站点中，所有的文件都存放在作为根目录的主目录中，这就使其他访问者对用户 FTP 站点中的文件查找变得非常方便。设置主目录与虚拟目录的操作步骤参照上一小节 Web 服务器的配置。

1. 创建 FTP 站点

创建 FTP 站点的操作步骤如下：

首先，打开“Internet 信息服务”管理器窗口，展开服务器节点。右击“默认 FTP 站点”，从弹出的快捷菜单中选择“新建”→“站点”命令，打开“FTP 站点创建向导”对话框。

然后，单击“下一步”按钮，打开“IP 地址和端口设置”对话框，如图 12-12 所示。在“IP 地址”下拉列表框中选择或直接输入 IP 地址；在“TCP 端口”文本框中输入 TCP 端口值，默认值为 21。

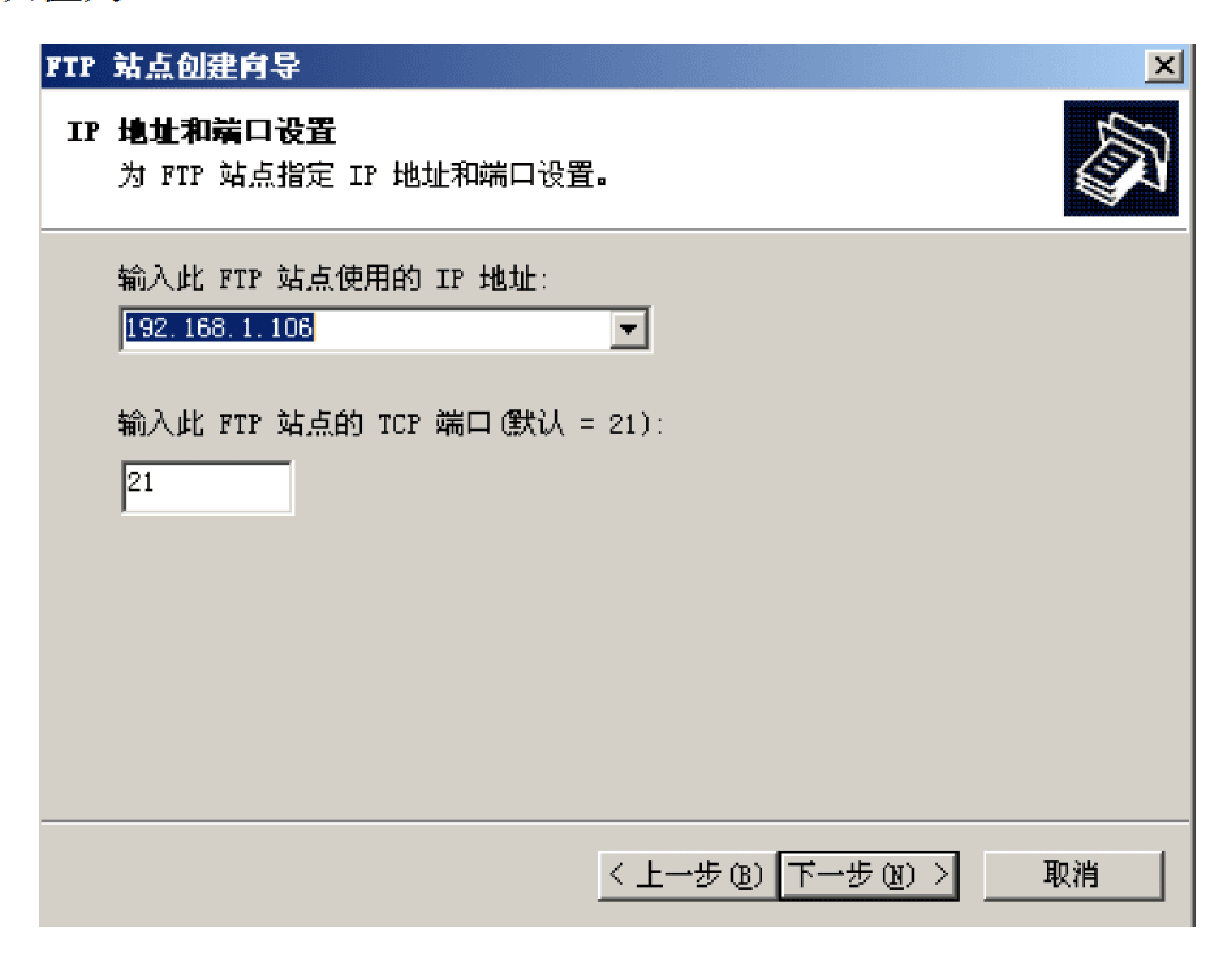


图 12-12 设置 IP 地址和端口

在图 12-12 中，单击“下一步”按钮，打开“FTP 站点主目录”对话框，如图 12-13 所示。在“路径”中，输入主目录的路径，或单击“浏览”按钮，选择路径。

在图 12-13 中，单击“下一步”按钮，打开“FTP 站点访问权限”对话框，如图 12-14 所示。在“允许下列权限”选项组中，设置主目录的访问权限。

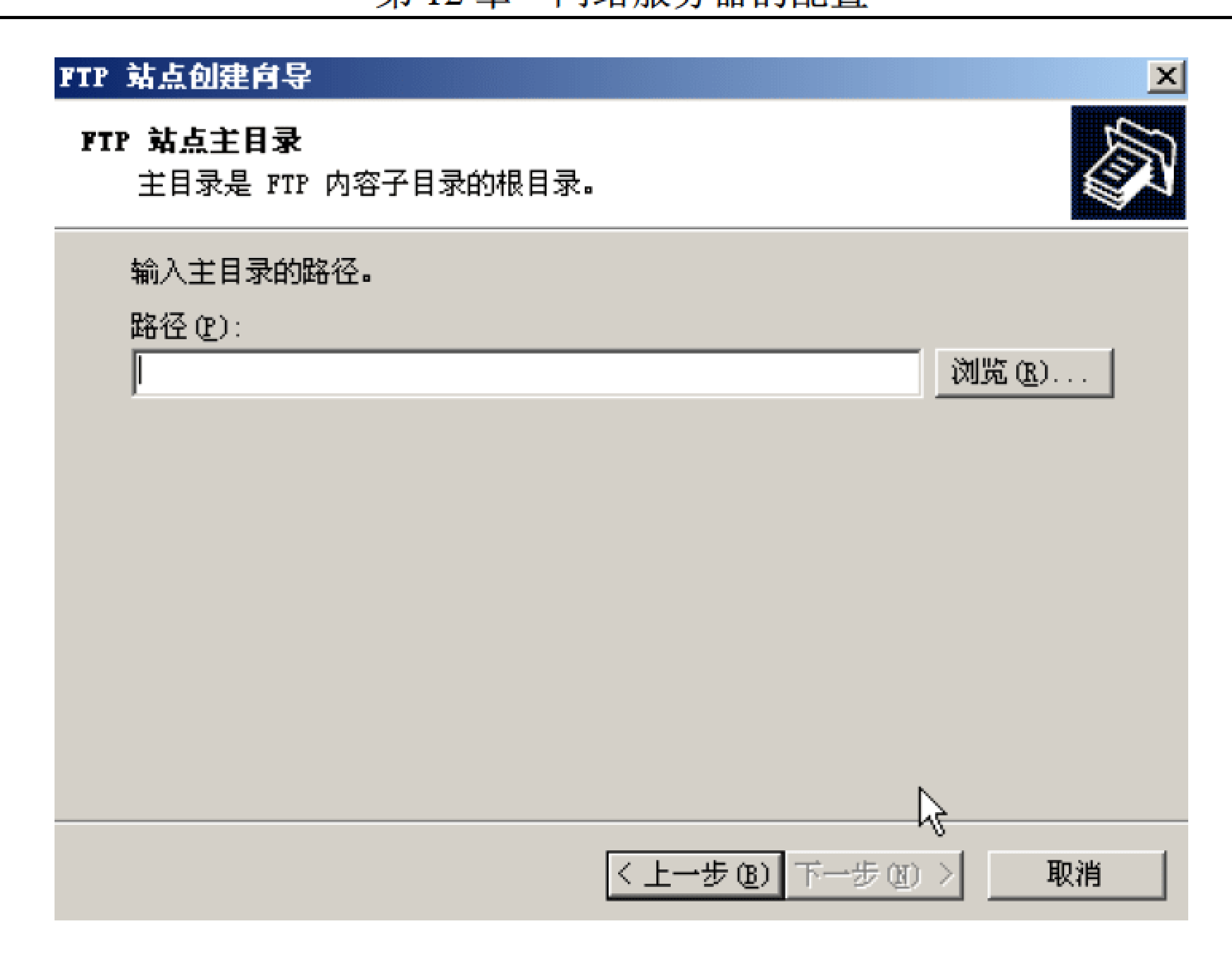


图 12-13　输入站点主目录和路径

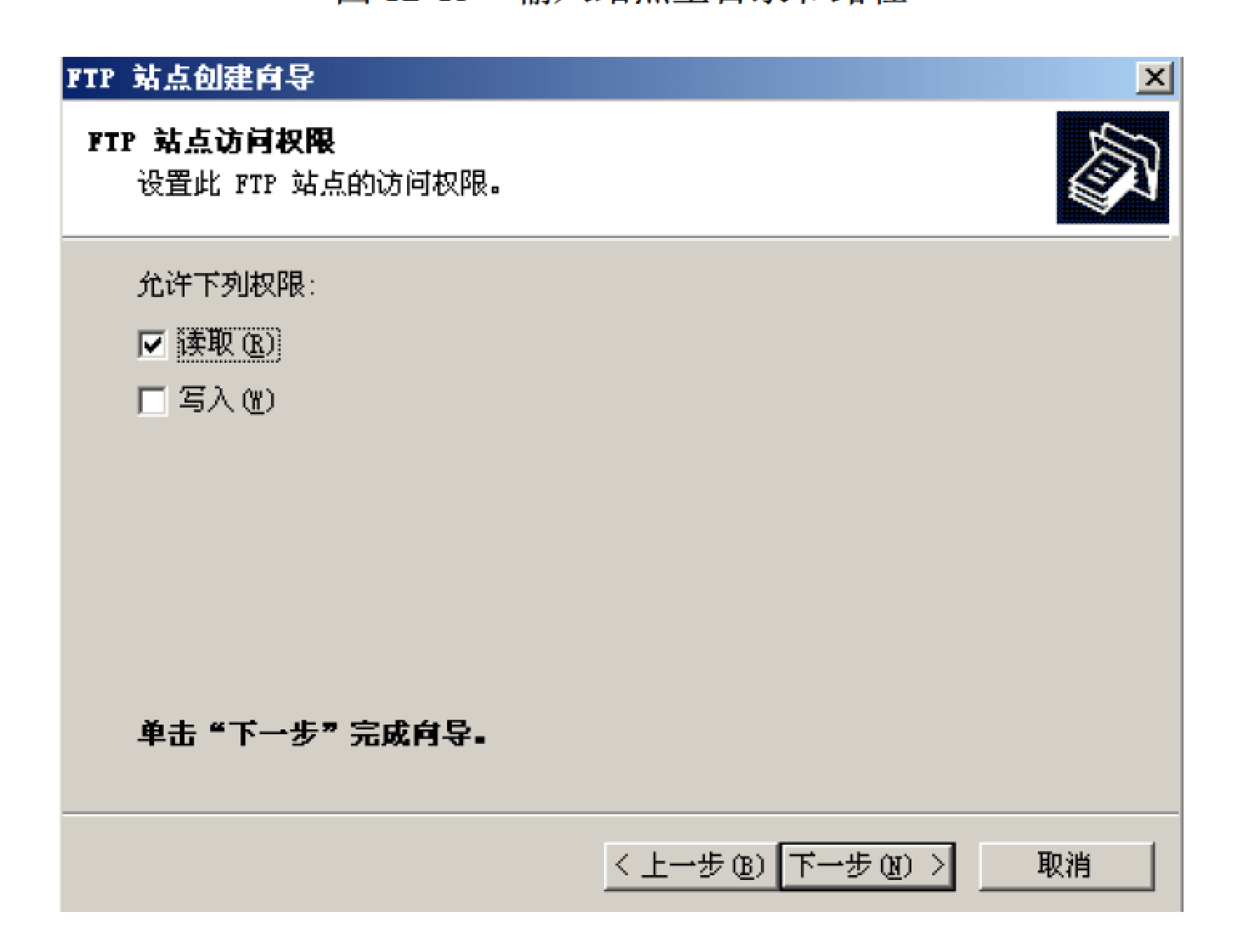


图 12-14　设置主目录的访问权限

2．访问安全设置

FTP 站点的安全相当重要，Windows Server 2003 中对 FTP 服务器可配置用户身份认证、限制访问 FTP 的 IP 地址，从而保证 FTP 的安全。

（1）禁止匿名访问。禁止匿名访问在属性信息的“安全账户”选项卡中设置。默认情况下 FTP 允许用户匿名访问，如果站点安全性要求较高，取消选中“允许匿名连接”即可禁止用户匿名访问该FTP，如图 12-15所示。

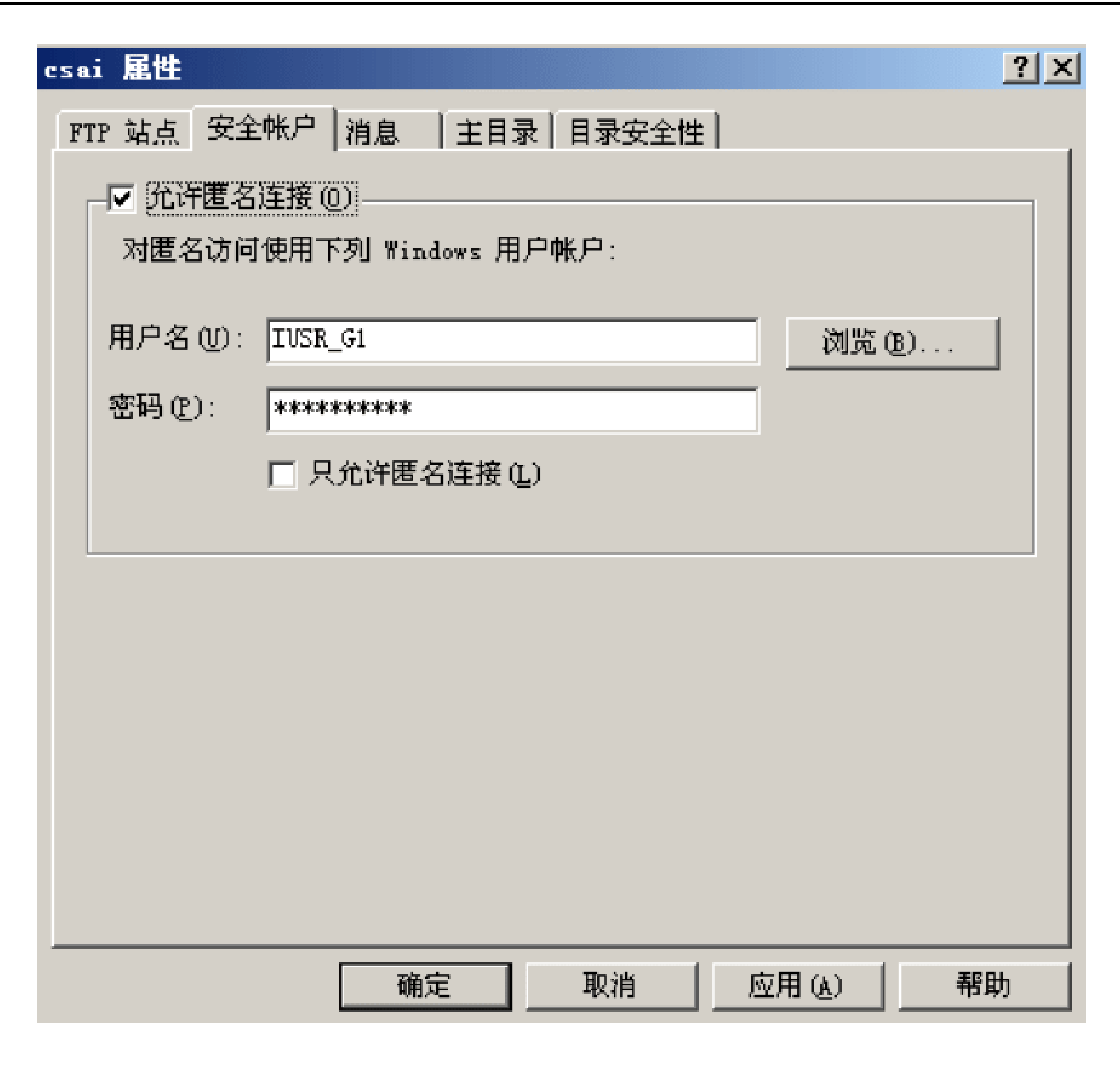


图 12-15 匿名连接设置

（2）限制 IP 地址。限制 IP 地址在属性信息的“目录安全性”选项卡中设置。通过对 IP 地址的限制可以只允许指定范围内的计算机访问该 FTP 站点，从而避免外界恶意攻击，如图 12-16 所示。

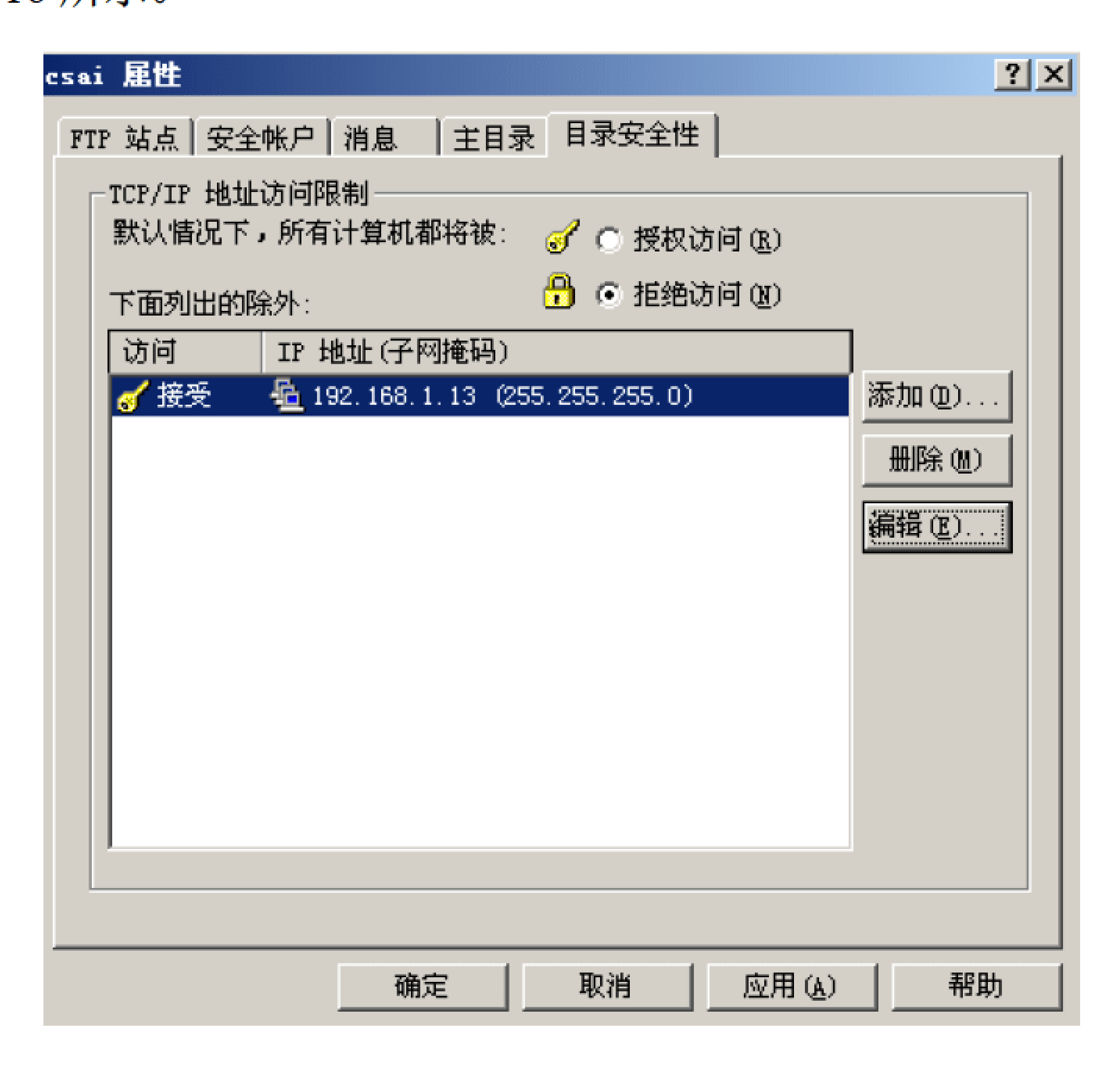


图 12-16 限制 IP 访问设置

3．常见 FTP 客户端操作命令

FTP> !：从 ftp 子系统退出到外壳。

FTP> ?：显示 ftp 命令说明。? 与 help 相同。

格式：? [command]

说明：

[command]指定需要帮助的命令名称。如果没有指定 command，ftp 将显示包含全部命令的列表。

FTP> cd：更改远程计算机上的工作目录。

格式：cd remote-directory

说明：

remote-directory 指定要更改的远程计算机上的目录。

FTP> delete：删除远程计算机上的文件。

格式：delete remote-file

说明：

remote-file 指定要删除的文件。

FTP> dir：显示远程目录文件和子目录列表。

格式：dir [remote-directory] [local-file]

说明：

remote-directory 指定要查看其列表的目录。如果没有指定目录，将使用远程计算机中的当前工作目录。local-file 指定要存储列表的本地文件。如果没有指定，输出将显示在屏幕上。

FTP> get：使用当前文件转换类型将远程文件复制到本地计算机。

格式：get remote-file [local-file]

说明：

remote-file 指定要复制的远程文件。local-file 指定要在本地计算机上使用的名称。如果没有指定，文件将命名为 remote-file。

FTP >put：使用当前文件传送类型将本地文件复制到远程计算机上。

格式：put local-file [remote-file]

说明：

local-file 指定要复制的本地文件。remote-file 指定要在远程计算机上使用的名称。如果没有指定，文件将命名为 local-file。

FTP >pwd：显示远程计算机上的当前目录。

FTP >quit：结束与远程计算机的 FTP 会话并退出 ftp。

12.3　DNS 服务器配置

本考点主要介绍了 DNS 服务相关概念、工作原理，以及在 Windows/Linux 下 DNS

服务器的具体配置方法。

12.3.1 DNS 基础知识

本节简单介绍 DNS 的基础知识，包括 DNS 服务器的分类，以及相关的术语。

1．DNS 服务器的类型

DNS 服务器可以分为主域名服务器、辅助域名服务器、高速缓存服务器、转发域名服务器四类。

1）主域名服务器（Primary Name Server）

主域名服务器负责维护这个区域的所有域名信息，是特定域所有信息的权威性信息源。一个域有且只有一个主域名服务器，它从域管理员构造的本地磁盘文件中加载域信息，该文件（区文件）包含着该服务器具有管理权的一部分域结构的最精确信息。主服务器是一种权威性服务器，因为它以绝对的权威去回答对其域的任何查询。

配置主域名服务器需要一整套配置文件，包括正规域的区文件（named.hosts）和反向域的区文件（named.rev）、引导文件（named.conf）、高速缓存（named.ca）和回送文件（named.local），其他的配置都不需要这样一整套文件。

2）辅助域名服务器（Secondary Name Server）

辅助域名服务器当主域名服务器关闭、出现故障或负载过重的时候，可从主域名服务器中转移一整套域信息。区文件是从主服务器中转移出来的，并作为本地磁盘文件存储在辅助服务器中。这种转移称为“区文件转移”。在辅助域名服务器中有一个所有域信息的完整复制，可以权威地回答对该域的查询，因此，辅助域名服务器也称作权威性服务器。

配置辅助域名服务器不需要生成本地区文件，因为可以从主服务器中下载该区文件。然而其他的文件是需要的，包括引导文件、高速缓存文件和回送文件。

3）高速缓存服务器（Caching-only Server）

高速缓存服务器又称为唯高速缓存服务器，可运行域名服务器软件但是没有域名数据库软件。它从某个远程服务器取得每次域名服务器查询的回答，一旦取得一个答案，就将它放在高速缓存中，以后查询相同的信息时就用它予以回答。所有的域名服务器都按这种方式使用高速缓存中的信息，但唯高速缓存服务器则依赖于这一技术提供所有的域名服务器信息。唯高速缓存服务器不是权威性服务器，它提供的所有信息都是间接信息。

对于唯高速缓存服务器只需要配置一个高速缓存文件，但最常见的配置还包括一个回送文件，这或许是最常见的域名服务器配置。接着才是唯转换程序配置，它是最容易配置的。

4）转发域名服务器（Forwarding Server）

转发域名服务器负责所有非本地域名的本地解析。

2．DNS 常用术语

DNS 是一个很复杂的概念，表 12-1 列出了常用的 DNS 术语。

表 12-1　常用 DNS 术语表

术　语	描　述
域	代表网络一部分的逻辑实体或组织
域名	主机名的一部分，它代表包含这个主机的域，它可以和域交换使用
主机	有时也称“节点”，网络上的一台计算机
域名服务器	提供 DNS 服务的计算机，它将 DNS 名字转化为 IP 地址
解析	把一个 DNS 服务器转化为与其相映的 IP 地址的过程
解析器	从域名服务器中提取 DNS 信息的程序或库子程序
反向解析	将给出的 IP 地址转化为其相映的 DNS 名字
欺骗	使网络看上去好像具有不同的 IP 地址或域名的行为

DNS 区域：其实是一个数据库，它提供 DNS 名称和相关数据，如 IP 地址和网络服务间的映射等。

（1）正向搜索区域：正向搜索区域使得 DNS 服务器能够向前查找，对于 DNS 服务器，必须配置至少一个正向搜索区域以便 DNS 服务器工作。

（2）反向搜索区域：把计算机的 IP 地址映射到对用户友好的域名，反向搜索区域并不是必要的，正向搜索区域也能够支持反向查找。

3．DNS 服务工作过程

下面简单讨论下域名的解析过程。这里要注意两点。

（1）主机向本地域名服务器的查询一般都是采用递归查询。所谓递归查询就是：如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查询请求报文（即替该主机继续查询），而不是让该主机进行下一步的查询。因此，递归查询返回的查询结果或者是所要查询的 IP 地址，或者是报错，表示无法查询到所需的 IP 地址。

（2）本地域名服务器向根域名服务器的查询通常都是迭代查询。迭代查询的特点是：当根域名服务器收到本地域名服务器发出的迭代查询请求报文时，要么给出所要查询的 IP 地址，要么告诉本地域名服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让本地域名服务器进行后续的查询（而不是替本地域名服务器进行后续的查询）。根域名服务器通常把自己知道的顶级服务器的 IP 地址告诉本地域名服务器，让本地域名服务器再向顶级域名服务器查询。顶级域名服务器在收到本地域名服务器的查询请求后，要么给出所查询的 IP 地址，要么告诉本地域名服务器下一步应当向哪一个权限域名服务器

进行查询。本地域名服务器就这样进行迭代查询。最后，知道了所要解析的域名的 IP 地址，然后把这个结果返回给发起查询的主机。当然，本地域名服务器也可以采用递归查询。这取决于最初的查询请求报文的设置是要求使用哪一种查询方式。

12.3.2 Windows 平台下 DNS 服务配置

本节具体介绍在 Windows 系统下，如何配置 DNS。

1. DNS 服务器的安装

默认情况下 Windows 2003 并没有安装 DNS 服务器组件，DNS 服务器安装步骤如下：

（1）选择“开始”→“程序”→“管理工具”→“配置您的服务器向导”命令。在打开的“向导”页中单击“下一步”按钮，如图 12-17 所示。

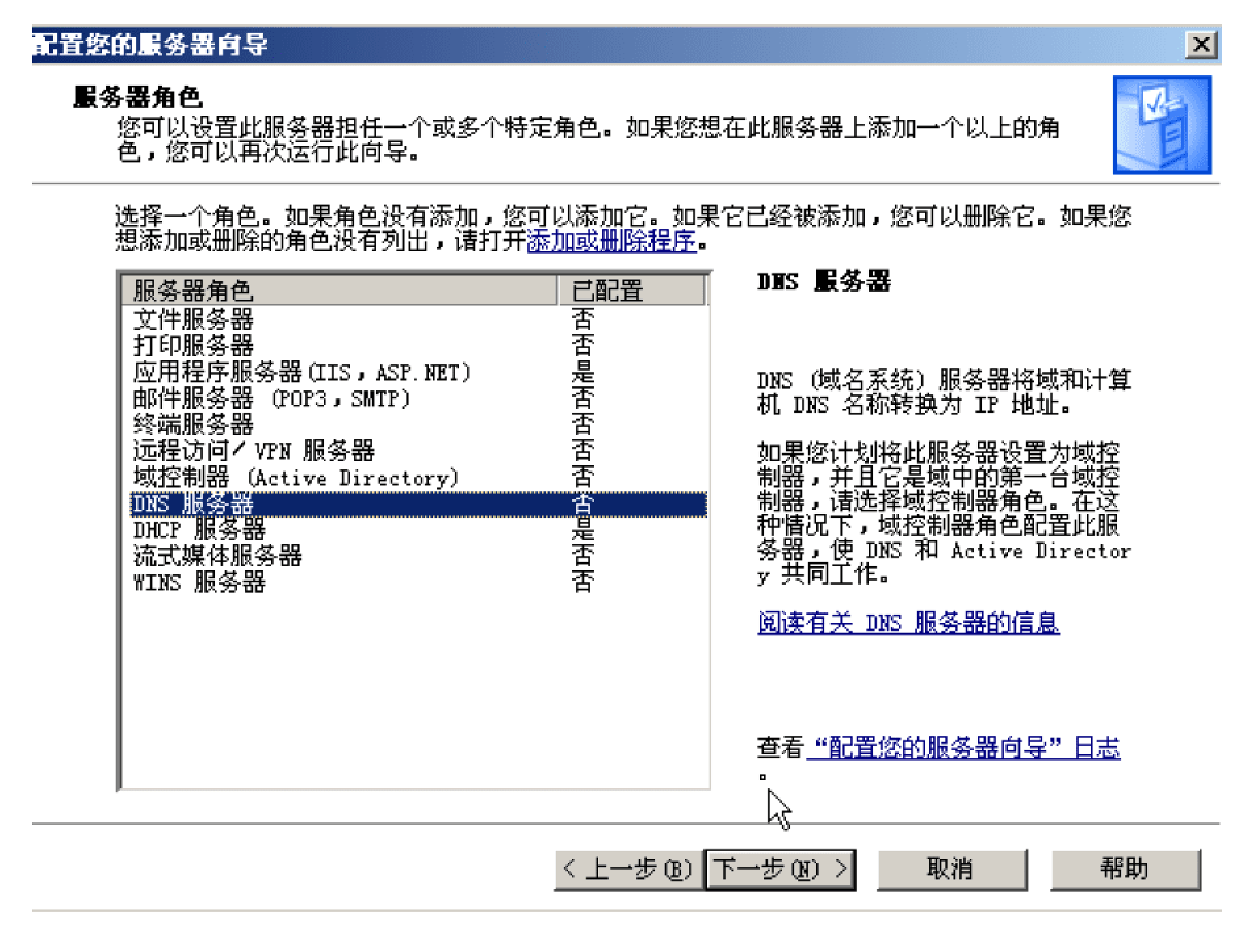


图 12-17 配置您的服务器向导

（2）向导开始安装 DNS 服务器组件，并可能会提示需要插入 Windows 2003 系统光盘或指定源文件，按照提示即可完成 DNS 服务器组件的安装。

2. 创建 DNS 解析区域

DNS 服务器组件安装好以后，会自动打开“配置 DNS 服务器向导”对话框，用户可在该向导指引下完成 DNS 服务器的配置。

（1）创建正向查找区域

单击“操作”→“新建区域”命令，系统启动“新建区域向导”对话框，如图 12-18

所示，该向导将引导用户创建新区域。

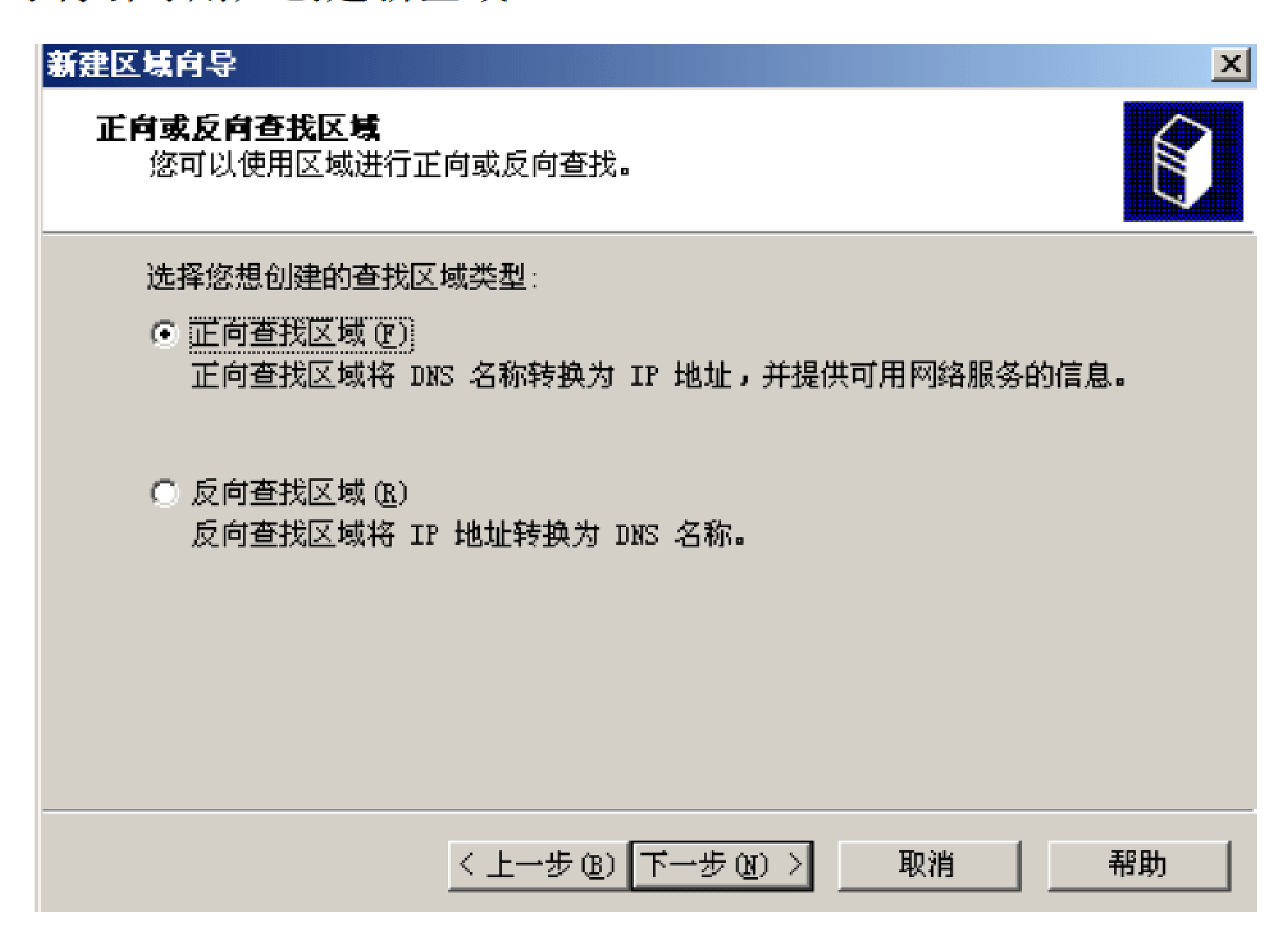


图 12-18　新建区域向导

单击“下一步”按钮弹出“区域名称”对话框，如图 12-19 所示，该对话框要求用户输入新建区域的名称。



图 12-19　新建区域名称

单击“下一步”按钮弹出“区域文件”对话框，如图 12-20 所示。

新建区域向导

区域文件
您可以创建一个新区域文件和使用从另一个 DNS 服务器复制的文件。

您想创建一个新的区域文件，还是使用一个从另一个 DNS 服务器复制的现存文件?

创建新文件，文件名为(C):

csai.cn.dns

使用此现存文件(U):

要使用此现存文件，请确认它已经被复制到该服务器上的 %SystemRoot%\system32\dns 文件夹，然后单击“下一步”。

< 上一步(B) 下一步(N) > 取消 帮助

图 12-20　区域文件名

区域数据库文件名默认与区域名相同，并以 dns 为扩展名，如 csai.cn.dns。当从另一台服务器移植区域到本服务器时，必须把区域文件存放到本服务器的 Winnt\System32\Dns 文件夹中。单击“下一步”按钮弹出“正在完成新建区域向导”对话框，该对话框显示出新区域的设置信息。如果信息正确，单击“完成”按钮，完成创建新区域的操作。在 DNS 右侧窗格中就显示出如图 12-21 所示的信息。

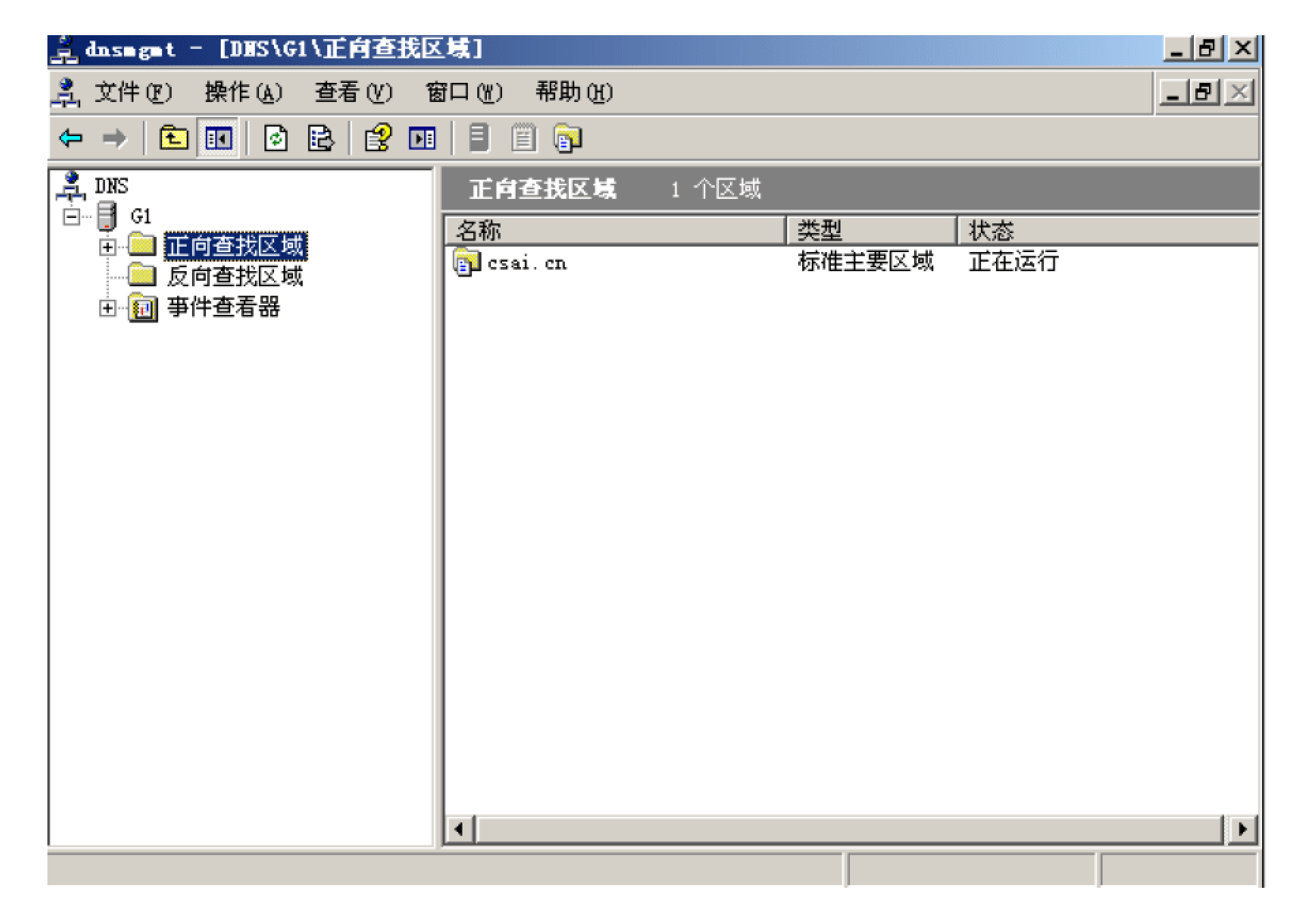


图 12-21　正向查找区域完成

（2）创建反向查找区域。

Windows 2000 DNS 服务器在安装 DNS 时会自动增加三个从 IP 地址到域名映射的反向搜索区域，它们是 0.in-addr.arpa、127.in-addr.arpa 和 255.in-addr.arpa。

创建反向搜索区域的操作步骤如下：

首先，前面步骤参见正向区域相对应的，在图 12-18 中，选中“反向搜索区域”单选按钮。

图 12-22 所示的对话框要求用户输入反向搜索区域的网络标识或区域名称。例如，在“网络 ID”文本框中输入 192.168.0，表示网络中的所有反向搜索都在这个新区域中解析，而反向搜索区域的文件名默认取自网络标识，由反向 IP 地址并增加 in-addr.arpa 后缀组成。

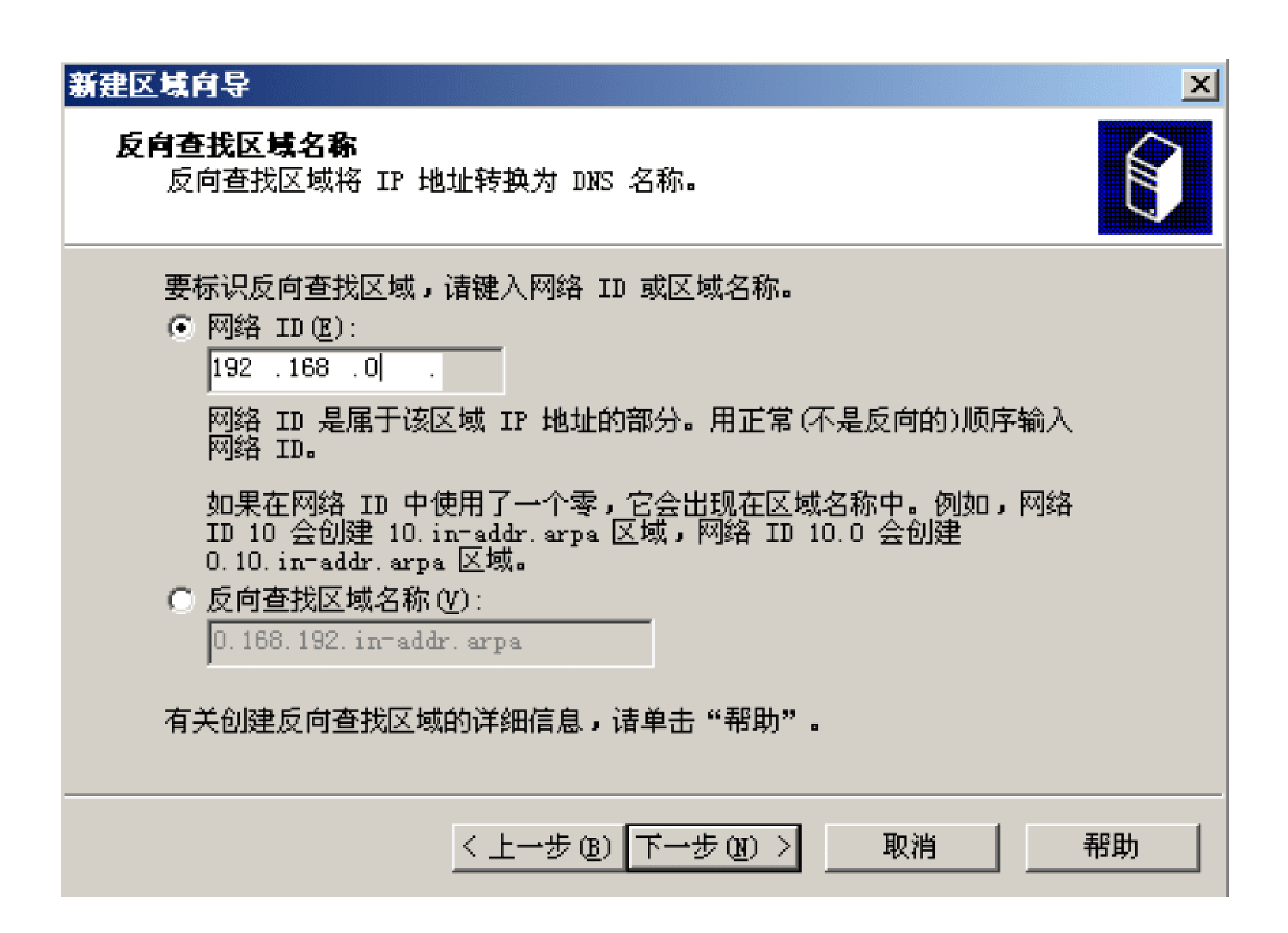


图 12-22　反向查找区域设置

单击“下一步”按钮弹出“区域文件”对话框，如图 12-23 所示。

该对话框要求用户输入反向搜索区域的数据库文件名，文件名默认为区域名加上 dns 扩展名，在这使用系统的默认值。

在图 12-23 中，单击“下一步”按钮，弹出“正在完成新建区域向导”对话框，对话框中显示出新区域的设置信息。单击“完成”按钮，就完成了创建新区域的操作。如图 12-24 所示。

3．创建域名

向导成功创建了 csai.cn 区域，还需要在此基础上创建指向不同主机的域名才能提供

域名解析服务。具体操作如下：

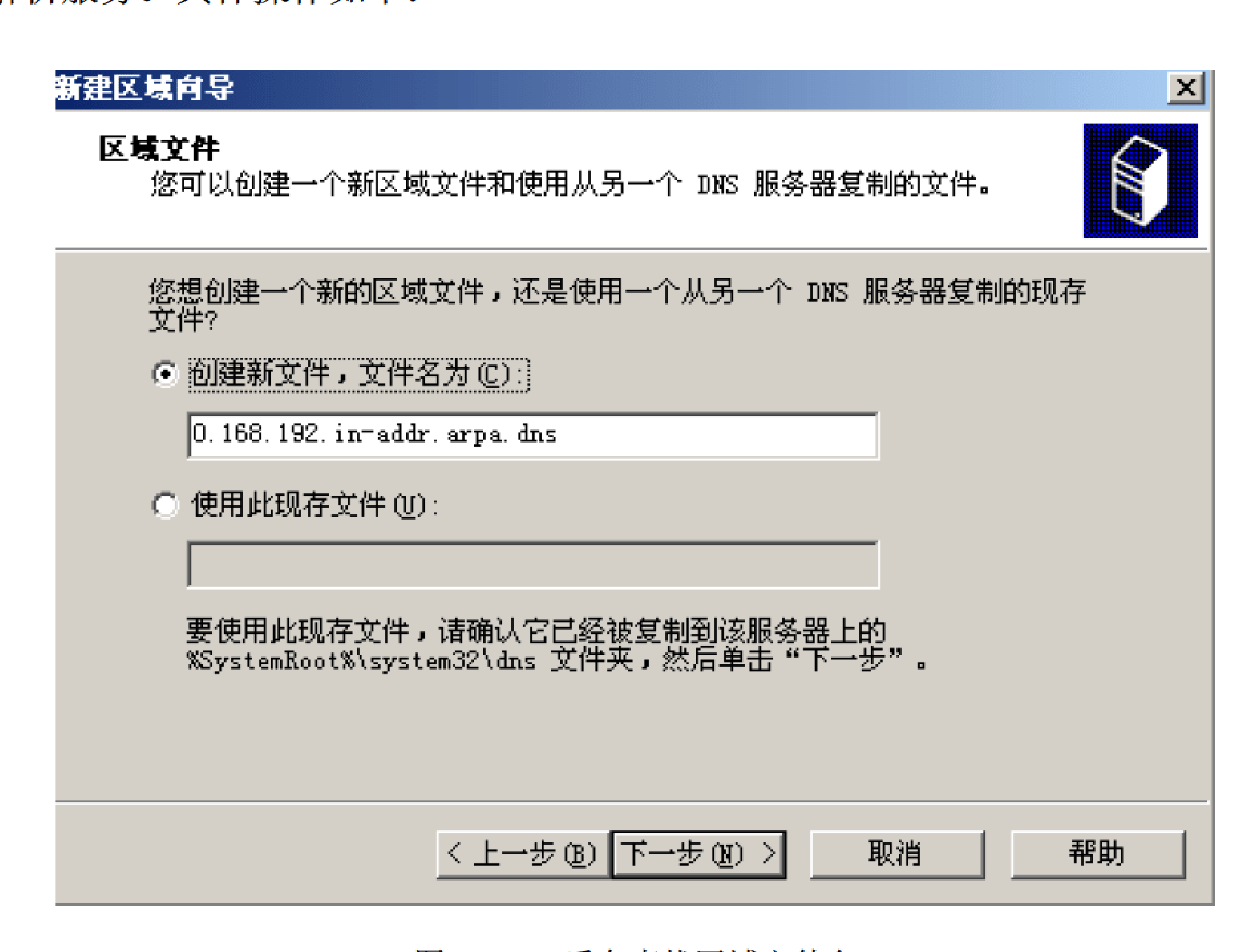


图 12-23 反向查找区域文件名

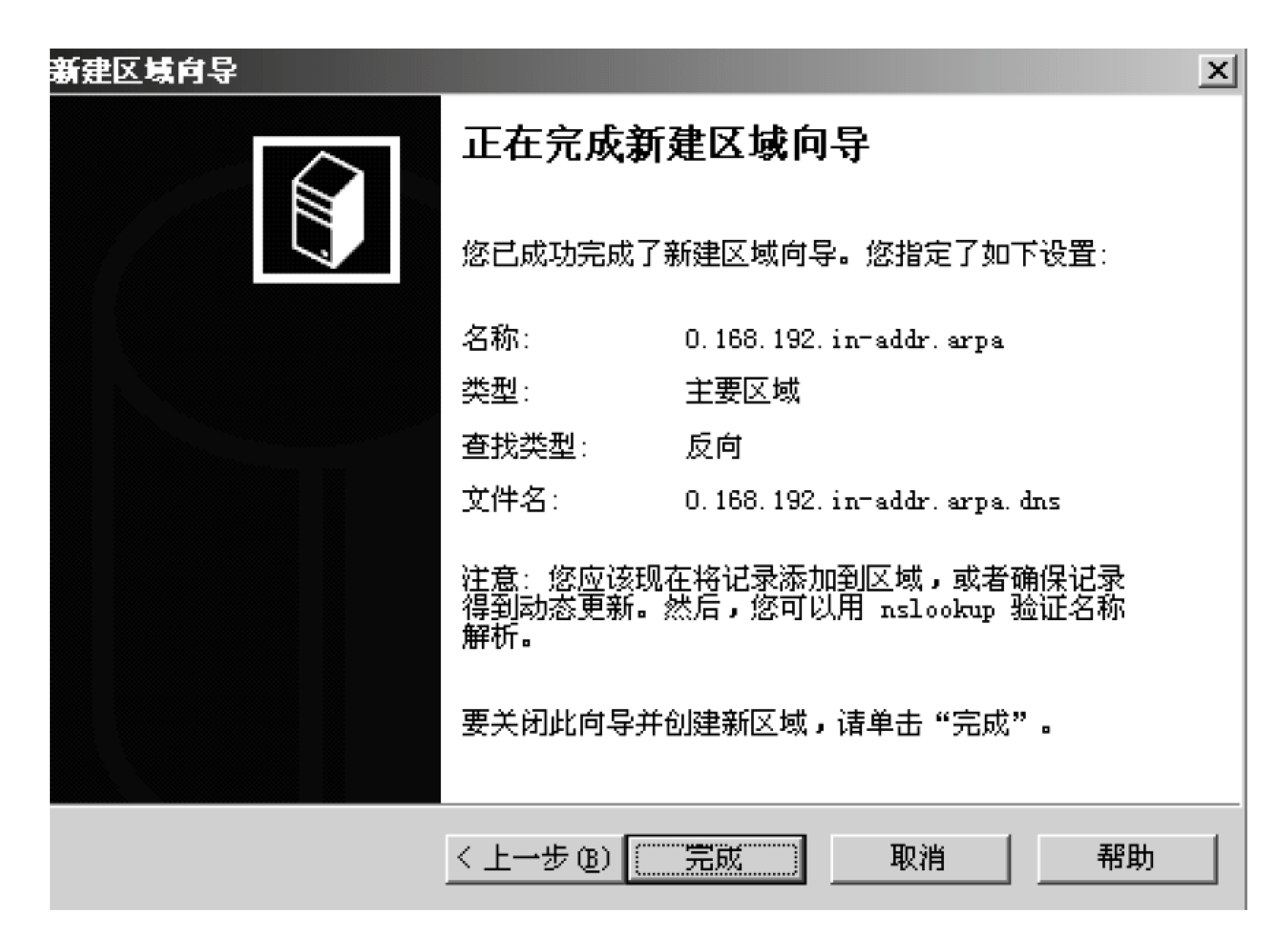


图 12-24 完成反向查找区域设置

（1）选择“开始”→“程序”→“管理工具”→“DNS 菜单”命令。打开 dnsmagt 控制窗口。

（2）在左窗格“正向查找区域”目录中，选择 csai.cn 区域，单击鼠标右键，选择“新建主机”命令。

打开如图 12-25 所示的“新建主机”对话框，在“名称”编辑框中输入一个能代表该主机提供服务的名称（本例中输入“www”），在“IP 地址”编辑框中输入该主机的 IP 地址（本例中输入“192.168.1.106”），单击“添加主机”按钮，很快提示完成主机记录的创建。

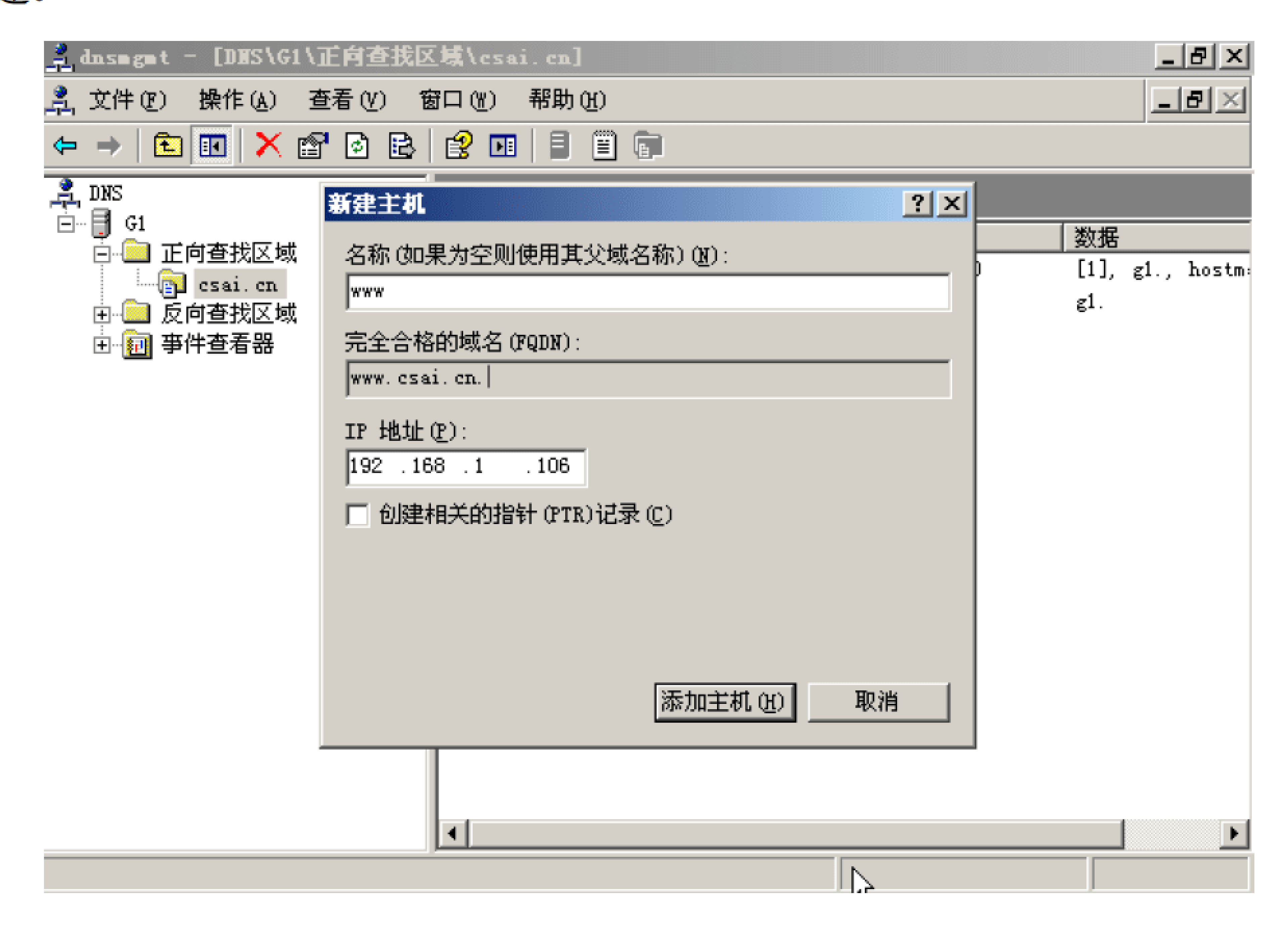


图 12-25　新建主机

12.3.3　Linux 平台下 DNS 服务配置

Linux 下架设 DNS 服务器通常是使用 BIND 程序来实现的。BIND 是一个客户/服务系统，又称为转换程序（resolver），它产生域名信息的查询，将这类信息发送给服务器，DNS 软件回答转换程序的查询。BIND 的服务方面是一个称为 named 的守护进程。

1．host.conf 文件解析

/etc/host.conf 是用来控制本地转换程序设置的文件。该文件告诉转换程序使用哪些服务、按照什么顺序进行。该文件的字段可以用空格或制表符分隔。字符“#”表示注释行。表 12-2 是可在 host.conf 中指定的选项。

表 12-2　/etc/host.conf 文件的配置选项

选　　项	说　　明
order	指定按照哪种顺序来尝试不同的名字解析机制。按列出的顺序来进行指定的解析服务。支持下面的名字解析机制： hosts 试图通过查找本地/etc/hosts 文件来解析名字 bind 使用 DNS 域名服务器来解析名字 nis 使用网络信息服务（NIS）协议来解析主机名字
multi	以 off 和 on 为参数。与 host 查询一起使用，用来确定一台主机是否在/etc/hosts 文件中指定了多个 IP 地址
nospoof	如果用逆向解析找出与指定的地址匹配的主机名，对返回的地址进行解析以确认它确实与您查询的地址相配。为了防止“骗取”IP 地址，通过指定 nospoofon 来允许这种功能
alert	以 off 和 on 为参数。如果打开，任何试图骗取 IP 地址的行为都通过 syslog 工具进行记录
trim	以域名为参数。在/etc/hosts 中查找名字前，trim 删除这个域名。这使你只把基本主机名放在/etc/host.conf 中而不指定域名

下面这个例子是主机 vlager 上的/etc/host.conf 文件：

```
#/etc/host.conf
#We have named running, but no NIS(yet)
order bind hosts
#Allow multip lead drs
multion
#Guard against spoof attempts
nospoofon
#Trim local domain (not really necessary).
trimvbrew.com.
```

这个例子给出了域 vbrew.com 的通用解析程序配置。该解析程序首先使用 DNS，然后使用/etc/hosts 文件查找主机名。在解析查找中指定本地/etc/hosts 文件是一个可靠的选择。如果由于某种原因不能使用域名服务器，我们还可以使用主机文件中列出的那些主机名。

2．resolv.conf 文件解析

当配置转换程序使用 BIND 域名服务查询主机时，我们必须告诉转换程序使用哪一个域名服务器。用来完成这项任务的工具就是/etc/resolv.conf 文件。/etc/resolv.conf 控制转换程序使用 DNS 解析主机名使用的方式，并且它可以明确地定义系统的配置，允许我们命名由于默认服务器不响应而使用的备份服务器。在/etc/resov.conf 中使用的命令，具有系统专用的形式，但一般都支持 domain 和 nameserver 两项命令。

（1）nameserver 项。利用 IP 地址让转换程序去识别查询域信息的那些服务器。我们

可以多次使用 nameserver 选项，可以使用多达三个域名服务器。这些域名服务器是按照它们在文件中的顺序进行查询的，如果没有接收到一个服务器的响应，就去试表中的下一个服务器，直到所有服务器试完为止（如果在/etc/resolv.conf 文件中设置了三个以上的域名服务器，那么，即使前三个服务器都没有响应查询请求，Linux 也不会去请求后面的服务器）。我们应该将最可靠的域名服务器列在最前面，以便在查询时不会超时。

（2）domain 项。用来定义默认域名（主机的本地域名）。转换程序会将默认域名挂在任何不含点的主机名后面。例如，转换程序接收到主机名 vale（它不含点），就将其默认域名挂接在 vale 后面，构成对它的查询。如果 domian 域中的 name 值是 vbrew.com，那么转换程序就将查询 vale.vbrew.com。我们可以看看下面这个例子，这是 VirtualBrewery 中的 resolv.conf 文件：

```
#/etc/resolv.conf
#Our domain
domain vbrew.com
#We use vlager as central name server:
name server191.72.1.1
```

在该例中，通过 domain 指定默认域名，并列出一个用于解析主机名的域名服务器。在这个例子中没有指定查寻顺序（使用 search 选项），因此如果要查询一台机器的地址（如 vale），解析器则首先试图查找 vale，如果没找到，则查找 vale.vbrew.com，然后再查找 vbrew.com。

3．设置域名服务器

在 Linux 上的域名服务是由 named 守护进程来执行的，为了运行 named，只要在命令行中输入：

```
#/etc/rc.d/init.d/named start
```

虽然转换程序的配置只需要一个配置文件，但是在配置 named 时却要使用多个文件，一整套 named 配置文件如表 12-3 所示。

表 12-3　named 配置文件

配 置 文 件	说　　明
named.conf	设置一般的 named 参数，指向该服务器使用的域数据库信息的源，这类源可以是本地磁盘文件或远程服务器
named.ca	指向根域名服务器
named.local	用于在本地转换回送地址
named.hosts	将主机名映射为 IP 地址
named.rev	用于反向域的、将 IP 地址映射到主机名的区文件

named.conf 文件通常很小，只包括一些指向 DNS 信息源的信息。其中某些源是本地文件，其他则是远程服务器。下面我们将看一个需要生成所有文件类型的例子。

表 12-4 概括了 named.conf 文件中使用的各种配置语句，它提供的信息能帮助我们了解这些例子。

表 12-4　named.boot 文件的配置选项

选　项	说　明
Directory	指定 DNS 文件所在的目录。您可以重复此选项以指定几个不同的目录。可以给出这些目录相关的文件路径名
Master	以一个域名和一个文件名为参数。此选项声明 named 对指定的域具有控制权，并使 named 从指定的区域加载信息
Hint	为 named 建立高速缓存信息。以一个域名和一个文件名为参数。域名通常用“.”指定。指定的文件包括一组称为服务器提示的记录，这些记录列出了根域名服务器的信息
Forwarders	以一个域名服务器的列表作为参数。告诉本地域名服务器：如果它不能从它的本地信息中解析出地址，那么就与该列表中的服务器联系
Slave	把本地域名服务器变成一个从属服务器。如果给出了此选项，那么本地服务器就试着通过递归查询来解析 DNS 名字。它只把请求传递给 forwarders 选项行列出的服务器中的一个

配置 named.conf 文件所使用的方法即是控制将域名服务器，使其作为主服务器、辅助服务器，还是唯高速缓存服务器。理解不同配置的最佳方法是讨论各种 named.conf 的示例文件。

4．主服务器和辅助服务器的配置

虚构的 vbrew.com 是举例说明主服务器和辅助服务器的基础，下面是将 vlager 定义为 vbrew.com 域的主服务器的 named.conf 文件：

```
//generated by named-boot conf.pl
options{
directory "/var/named";
/*
*If there is a firewall lbetween you and name servers you want
*to talk to,you might need to uncomment the query-source
*directive below.Previous versions of BIND always asked
*questions using port 53 , but BIND 8.1 uses an unprivileged
*port by default.
*/
//query-source address *port 53;
};
//a caching only name server config
```

```
zone"."{
typehint;
file"named.ca";
};
zone"vbrew.com"{
type master;
file "named.hosts";
};
zone"0.0.127.in-addr.arpa"{
type master;
file "named.local";
};
zone"72.191.in-addr.arpa"{
type master;
file "named.rev";
};
```

上例中第一个 master 告诉我们这是 vbrew.com 域的主服务器。该域的数据是从 named.hosts 文件中加载的。在这个例子中，我们将文件名 named.hosts 作为区文件名，但也可以使用更有说明性的文字，例如，vbrew.com 区文件的名字使用 vbrew.com.hosts 则较好。

第三个 master 语句指向能将 IP 地址 191.72.0.0 映射为主机名的文件。它假定本地服务器是反向域 72.191.in-addr.arpa 的主服务器，该域的数据从文件 named.rev 中加载。

在上例配置中的 hint 语句和第二个用于回送域的 primary 语句我们前面在唯高速缓存配置中已经讨论过。在这些配置中，它们的作用是相同的，而且几乎在任何配置中都要使用它们。

辅助服务器的配置与主服务器的配置不同，它使用 slave 语句代替 master 语句。slave 语句指向用作域信息源的远程服务器，以替代本地磁盘文件。下面的 named.conf 文件可以将 vale 配置成为 vbrew.com 域的辅助服务器：

```
//generated by named-boot conf.pl
options{
directory "/var/named";
/*
*If there is a firewall between you and name servers you want
*to talk to,you might need toun comment the query-source
*directive below.Previous versions of BIND always asked
*questions using port 53,but BIND 8.1 uses an unprivileged
*port by default.
```

```
*/
//query-source address *port 53;
};
//acaching only name server config

zone"."{
typehint;
file"named.ca";
};
zone"0.0.127.in-addr.arpa"{
typemaster;
file"named.local";
};
zone"vbrew.com"{
typeslave;
file"named.hosts";
masters{191.72.1.3;};
};
zone"72.191.in-addr.arpa"{
typeslave;
file"named.rev";
masters{191.72.1.3;};
};
cache.named.ca
secondaryvbrew.com191.72.1.3named.hosts
secondary72.191.in-addr.arpa191.72.1.3named.rev
primary0.0.127.in-addr.arpanamed.local
```

第一个 slave 语句是使这个服务器成为 vbrew.com 的辅助服务器。它告诉 named 从 IP 地址为 191.72.1.3 的服务器中下载 vbrew.com 的信息，并将其数据保存在/var/named/named.hosts 文件中。

该配置文件中的下一行表示该本地服务器也是反向域 72.191.in-addr.arpa 的一个辅助服务器，而且该域的数据也从 191.72.1.3 中下载。该反向域的数据存储在 nameD.rev 中。

5．唯高速缓存服务器

配置唯高速缓存域名服务器是很简单的。必须有 named.conf 和 named.ca 文件，通常也要用到 named.local 文件。下面是用于唯高速缓存服务器的 named.conf 文件的例子，其中以“//”开头的是注释。

```
//generated by named-boot conf.pl
options{
directory "/var/named";
/*
*If there is a firewall between you and name servers you want
*to talk to,you might need toun comment the query-source
*directive below.Previous versions of BIND always asked
*questions using port 53,but BIND 8.1 uses an unprivileged
*portbydefault.
*/
//query-source address *port 53;
};

//a caching only name server config

zone "."{
type hint;
file"named.ca";
};
zone "0.0.127.in-addr.arpa"{
type master;
file "named.local";
};
```

directory 这一行告诉 named 到哪里去找寻文件。所有其后命名的文件都将是相对于此目录的。该文件告诉 named 去维持一个域名服务器响应的高速缓存，并利用 named.ca 文件的内容去初始化该高速缓存。该高速缓存初始化文件的名字可以是任何名字，但一般使用/var/named/named.ca。并不是在该文件中使用一个 hint 语句就能使它成为唯高速缓存配置，几乎每一种服务器的配置都要用到 cache 语句，而是因为没有 master 和 slave 语句才使它成为一个唯高速缓存配置。

但是，在我们这个例子中却有一个 master 语句。事实上，几乎在每一个唯高速缓存的配置文件中都有这一个语句，它将本地服务器定义为它自己的回送域的主服务器，并假定该域的信息存储在 named.local 文件中。这个回送域是一个 in-addr.arpa 域（in-addr.arpa 域用于指定逆向解析，或 IP 地址到 DNS 名字解析），它将地址 127.0.0.1 映射为名字 localhost。转换自己的回送地址对于大多数人都是有意义的，因为大多数的 named.conf 文件都包含这一项。

在大多数唯高速缓存服务器的配置文件中，这种 directory、master 和 hint 语句是唯一使用的语句，但也可以增加其他的语句，forwarders 和 slave 等语句都可以使用。

6. DNS 数据库文件和资源记录

配置 named 所需的所有文件（named.hosts、named.rev、named.local 和 named.ca）中的信息是以称为资源记录的形式存在的。每个资源记录都有一个类型，这个类型说明记录的功能。这些记录都是标准资源记录，称为 RR（Resource Records）。表 12-5 列出了最常见的资源记录类型。

表 12-5 常见标准资源记录

资源记录名	记录类型	功 能 说 明
地址	A	将主机名转换为地址。这个字段保存以点分隔的十进制形式的 IP 地址。任何给定的主机都只能有一个 A 记录，因为这个记录被认为是授权信息。这个主机的任何附加地址名或地址映射必须用 CNAME 类型给出
规范名	CNAME	给定一个主机的别名，主机的规范名字是在这个主机的 A 记录中指定的
主机信息	HINFO	描述主机的硬件和操作系统
邮件交换	MX	建立邮件交换器记录。MX 记录告诉邮件传送进程把邮件送到另一个系统，这个系统知道如何将它递送到它的最终目的地
名服务器	NS	标识一个域的域名服务器。NS 资源记录的数据字段包括这个域名服务器的 DNS 名。我们还需要指定这个名字服务器的地址与主机名相匹配的 A 记录
指针	PTR	将地址变换成主机名。主机名必须是规范主机名
管理开始	SOA	告诉域名服务器它后面跟着的所有所有资源记录是控制这个域的（SOA，表示授与控制权）。其数据字段用（）括起来并且通常是多行字段

12.4 电子邮件服务器配置

建立电子邮件服务器之前，要根据邮件服务器的提供服务的标准（如邮箱大小、网络带宽、最大支持用户数量、并发访问数量等）、网络管理员的技术水平和预算等情况，从硬件、软件、网络等几方面充分考虑，从而选取最佳方案。

电子邮件服务器主要负责邮件系统的存储转发工作，其提供服务的重要指标有：每个用户邮箱的大小、最大支持用户数量、最大支持并发用户访问数量等。

服务器的性能、网络支持能力、系统的稳定性、可靠性（容错、备份）、硬盘访问速度、硬盘支持的最大容量等在系统规划时需要提前考虑。即使当前投产系统对各项指标都要求不高，也要考虑到今后可能的拓展，在预算范围内，需要考虑的邮件服务器的一些指标如下：

（1）是否支持 CPU 扩展。

（2）是否支持磁盘阵列。

（3）是否支持增加硬盘。

（4）支持最大的硬盘容量。

（5）备份设备。

对于硬盘总容量的大小，将决定最终提供的用户数量和每个邮件用户的邮箱大小。扩展硬盘容量的方法中，小型应用基本上是靠在服务器内部增加硬盘来实现的，而对于大型邮件服务器来说，使用大容量硬盘柜则是最佳选择。

定期进行数据备份也是保证系统可靠性，提高系统服务水平所必需的，在经费许可的范围内，一定要购置备份设备，如磁带机、磁光盘机（MO）、刻录光盘（CDRW、DVDRW）驱动器等。

合适的硬件选择可以为避免重复投资或投资浪费。在系统设计之初没有充分考虑到系统可能的用户数量，在系统运行一段时间以后，系统硬件性能已经不能够满足需要时，如果是因为硬件不能够实现扩展而重新购置设备的话，将造成极大的浪费。

在网络管理员考试大纲中规定本节知识点主要了解 E-mail 相关的协议，掌握 IIS 下 E-mail 的配置方法，能够完成服务器的安装与配置。

E-mail 是 Internet 上使用最多的一种网络服务，与 E-mail 相关的有三个协议：

（1）SMTP：简单邮件传送协议，用于邮件的发送，工作在 25 号端口上。

（2）POP3：邮局协议 V3.0，用于接收邮件，工作在 110 号端口上。

（3）IMAP：邮件访问协议，是用于替代 POP3 协议的新协议，工作在 143 号端口上。

接下来我们设置邮件服务器。因为 IIS 提供 SMTP 虚拟服务器，所以可通过本地 SMTP 服务向外发送电子邮件。

（1）常规：设置好 SMTP 虚拟服务器，对于使用动态 IP 的用户而言，IP 地址还是设置为“全部未指定”。

（2）访问：设置“访问控制”、“安全通信”、“连接控制”以及“中继限制”等。

（3）邮件：限制邮件大小、会话大小、每个连接的邮件数和每个邮件的收件人数等，还可以将“死信”（无法投递的信件）保存到一定目录中。

（4）传递：设置邮件“出站”的相关参数，如“第一次重试间隔”、“第二次重试间隔”、“第三次重试间隔”等，还可以设置“出站安全性”、“出站连接”等。

12.5　DHCP 服务器配置

本考点主要介绍 DHCP 服务相关概念，工作原理及在 Windows/Linux 下 DHCP 服务器的具体配置方法。

12.5.1　DHCP 基础知识

本节主要介绍 DHCP 基础知识，包括配置 DHCP 服务器的优点、DHCP 服务器具体工作方式、三种为客户机分配地址的方式以及与 DHCP 服务相关的命令。

1．配置 DHCP 服务器的优点

配置 DHCP 服务器有如下优点：

（1）管理员可以集中为整个互联网指定通用和特定子网的 TCP/IP 参数，并且可以定义使用保留地址的客户机的参数。

（2）客户机不需手工配置 TCP/IP，因为 DHCP 提供了安全可信的配置。DHCP 避免了在每台计算机上手工输入数值引起的配置错误，还能防止网络上计算机配置地址的冲突。

（3）使用 DHCP 服务器能大大减少配置花费的开销和重新配置网络上计算机的时间，服务器可以在指派地址租约时配置所有的附加配置值。

（4）客户机在子网间移动时，旧的 IP 地址自动释放以便再次使用。在再次启动客户机时，DHCP 服务器会自动为客户机重新配置 TCP/IP。

（5）大部分路由器可以转发 DHCP 配置请求，因此，互联网的每个子网并不都需要 DHCP 服务器。

2．DHCP 服务器工作过程

DHCP 是基于客户机/服务器模型设计的，DHCP 客户和 DHCP 服务器之间通过收发 DHCP 消息进行通信，如图 12-26 所示。



图 12-26　DHCP 服务过程

其过程主要如下：首先需要 IP 地址的主机在启动时就向 DHCP 服务器广播发送发现报文（Dhcpdiscover）（将目的地址置为全 1，即 255.255.255.255），这时该主机就变成 DHCP 客户。发送广播报文是因为现在还不知道 DHCP 服务器在什么地方。这样，在本地网络上的所有主机都能够接收到这个广播报文，但只有 DHCP 服务器才对此广播报文进行回答。DHCP 服务器先在其数据库中查找该计算机的配置信息。若找到，则返回找到信息。若找不到，则从服务器的 IP 地址池中取一个地址分配给该计算机。DHCP 服务器的回答报文叫做提供报文（Dhcpoffer），表示“提供”了 IP 地址等配置信息。如果客户端收到网络上多台 DHCP 服务器的响应，只会挑选其中一个 Dhcpoffer（通常是最先抵达的那个），并且会向网络发送一个 Dhcprequest 广播封包，告诉所有 DHCP 服务器它将指定接受哪一台服务器提供的 IP 地址。当 DHCP 服务器接收到客户端的 Dhcprequest

之后，会向客户端发出一个 Dhcpack 响应报文，以确认 IP 租约的正式生效，也就结束了一个完整的 DHCP 工作过程。

3．DHCP 服务器分配地址方式

DHCP 服务器有三种为 DHCP 客户机分配 TCP / IP 地址的方式：

（1）手工分配：管理员在 DHCP 服务器通过手工方法配置 DHCP 客户机的 IP 地址。当 DHCP 客户机要求网络服务时，DHCP 服务器把手工配置的 IP 地址传递给 DHCP 客户机。

（2）自动分配：不需要进行任何的 IP 地址手工分配。当 DHCP 客户机第一次向 DHCP 服务器租用到 IP 地址后，这个地址就永久地分配给了该 DHCP 客户机，而不会再分配给其他客户机。

（3）动态分配：当 DHCP 客户机向 DHCP 服务器租用 IP 地址时，DHCP 服务器只是暂时分配给客户机一个 IP 地址。只要租约到期，这个地址就会还给 DHCP 服务器，以供其他客户机使用。如果 DHCP 客户机仍需要一个 IP 地址来完成工作，则可以再租用另外一个 IP 地址。

4．DHCP 相关命令

ipconfig 命令动态获取与释放 IP 地址：

（1）具体功能。

该命令用于显示所有当前的 TCP/IP 网络配置值、刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。使用不带参数的 IPCONFIG 可以显示所有适配器的 IP 地址、子网掩码、默认网关。

（2）语法详解。

ipconfig[/all][/renew[adapter][/release[adapter][/flushdns][/displaydns][/registerdns][/showclassid adapter] [/setclassid adapter [classID]

（3）参数说明。

/all 显示所有适配器的完整 TCP/IP 配置信息。在没有该参数的情况下 IPCONFIG 只显示 IP 地址、子网掩码和各个适配器的默认网关值。适配器可以代表物理接口（例如安装的网络适配器）或逻辑接口（例如拨号连接）。

/renew[adapter]更新所有适配器（如果未指定适配器），或特定适配器（如果包含了 adapter 参数）的 DHCP 配置。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上可用。要指定适配器名称，可键入使用不带参数的 IPCONFIG 命令显示的适配器名称。

/release[adapter]发送 DHCPRELEASE 消息到 DHCP 服务器，以释放所有适配器（如果未指定适配器）或特定适配器（如果包含了 adapter 参数）的当前 DHCP 配置并丢弃 IP 地址配置。该参数可以禁用配置为自动获取 IP 地址的适配器的 TCP/IP。要指定适配器名称，可键入使用不带参数的 IPCONFIG 命令显示的适配器名称。

/flushdns 清理并重设 DNS 客户解析器缓存的内容。如有必要，在 DNS 疑难解答期间，可以使用本过程从缓存中丢弃否定性缓存记录和任何其他动态添加的记录。

/displaydns 显示 DNS 客户解析器缓存的内容，包括从本地主机文件预装载的记录以及由计算机解析的名称查询而最近获得的任何资源记录。DNS 客户服务在查询配置的 DNS 服务器之前使用这些信息快速解析被频繁查询的名称。

/registerdns 初始化计算机上配置的 DNS 名称和 IP 地址的手工动态注册。可以使用该参数对失败的 DNS 名称注册进行疑难解答或解决客户和 DNS 服务器之间的动态更新问题，而不必重新启动客户计算机。TCP/IP 协议高级属性中的 DNS 设置可以确定 DNS 中注册了哪些名称。

/showclassid adapter 显示指定适配器的 DHCP 类别 ID。要查看所有适配器的 DHCP 类别 ID，可以使用星号（*）通配符代替 adapter。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上可用。

/setclassid adapter [classID]配置特定适配器的 DHCP 类别 ID。要设置所有适配器的 DHCP 类别 ID，可以使用星号（*）通配符代替 adapter。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上可用。如果未指定 DHCP 类别的 ID，则会删除当前类别的 ID。

注意：IPCONFIG 等价于 WINIPCFG，后者在 Windows 98/Me 上可用。尽管 Windows XP 没有提供像 WINIPCFG 命令一样的图形化界面，但可以使用“网络连接”查看和更新 IP 地址。要做到这一点，打开网络连接，右键单击某一网络连接，选择“状态”命令，然后选择“支持”选项卡。

该命令最适用于配置为自动获取 IP 地址的计算机。它使用户可以确定哪些 TCP/IP 配置值是由 DHCP、自动专用 IP 地址（APIPA）和其他配置配置的。

12.5.2 Windows 平台下 DHCP 服务配置

和安装 DNS 服务组件方法一样，安装完 DHCP 服务器后，用户在 DHCP 控制台窗口中，将看到添加服务器的图标、服务器的名称及地址，如图 12-27 所示。

1. 创建 DHCP 作用域

创建作用域的主要作用即是为服务器指定和配置好可分配的 IP 地址。因此，在创建新的 DHCP 服务器的操作中创建作用域的工作是至关重要的，它关系到 DHCP 是否拥有可分配的 IP 地址。

创建 DHCP 作用域的操作步骤如下：

首先，选择“开始”→“程序”→“管理工具”→DHCP 命令，打开 DHCP 控制台窗口。选择要创建作用域的 DHCP 服务器，选择“操作”→“新建作用域”命令，弹出“作用域名”对话框，如图 12-28 所示。作用域名能帮助用户快速识别有关的 IP 地址。

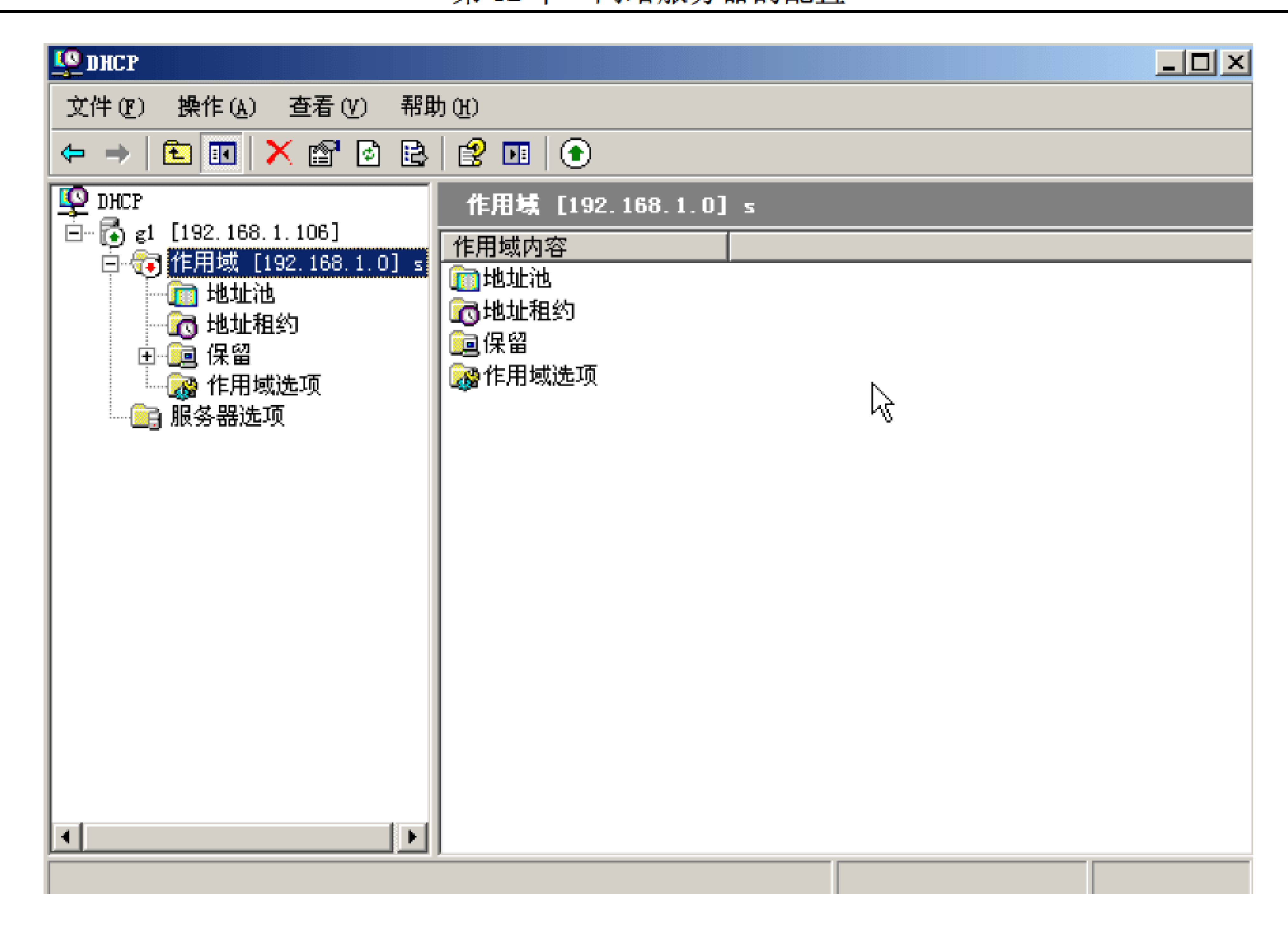


图 12-27　DHCP 控制台

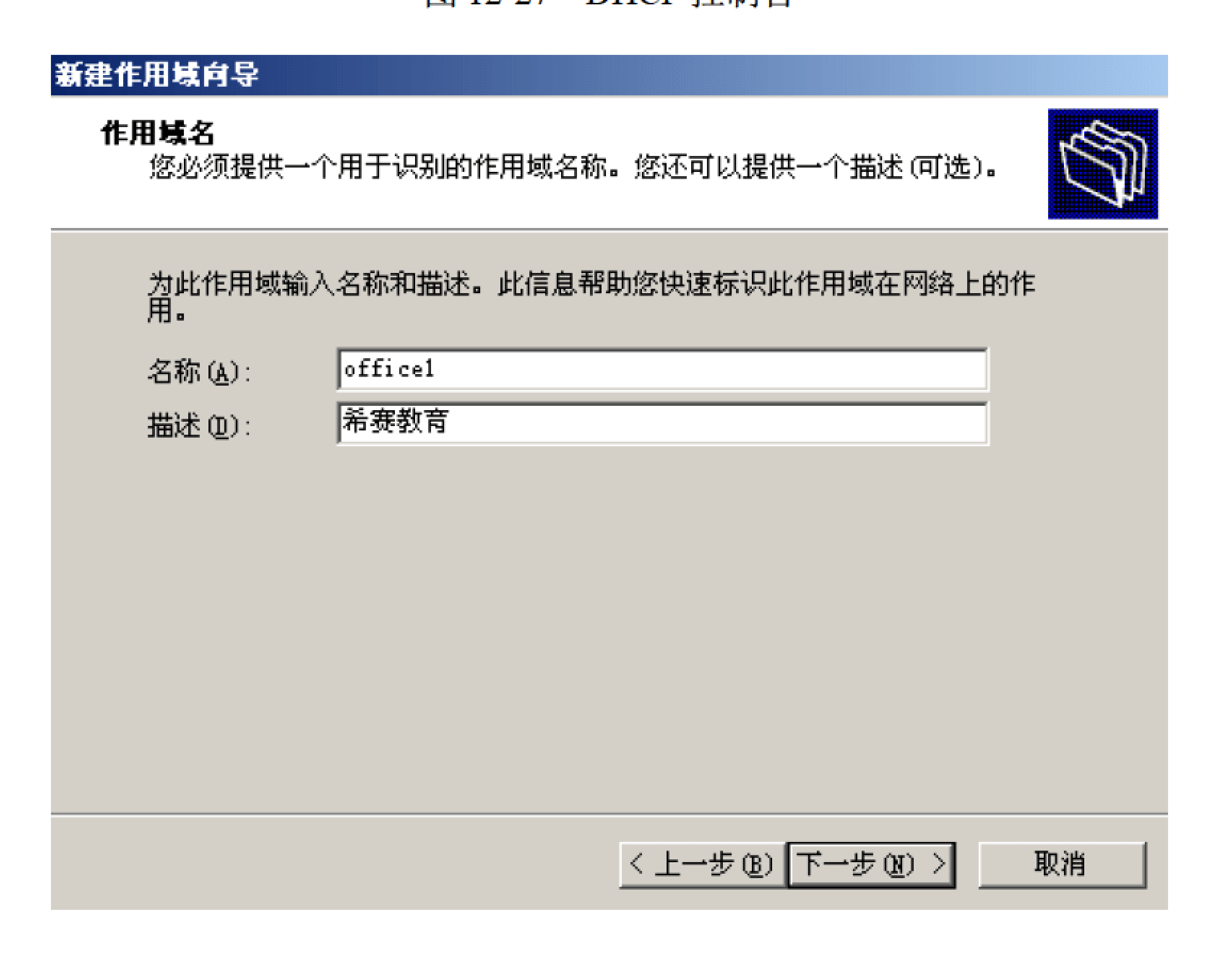


图 12-28　作用域名

在图 12-28 中，单击“下一步”按钮，弹出“IP 地址范围”对话框，如图 12-29 所示。

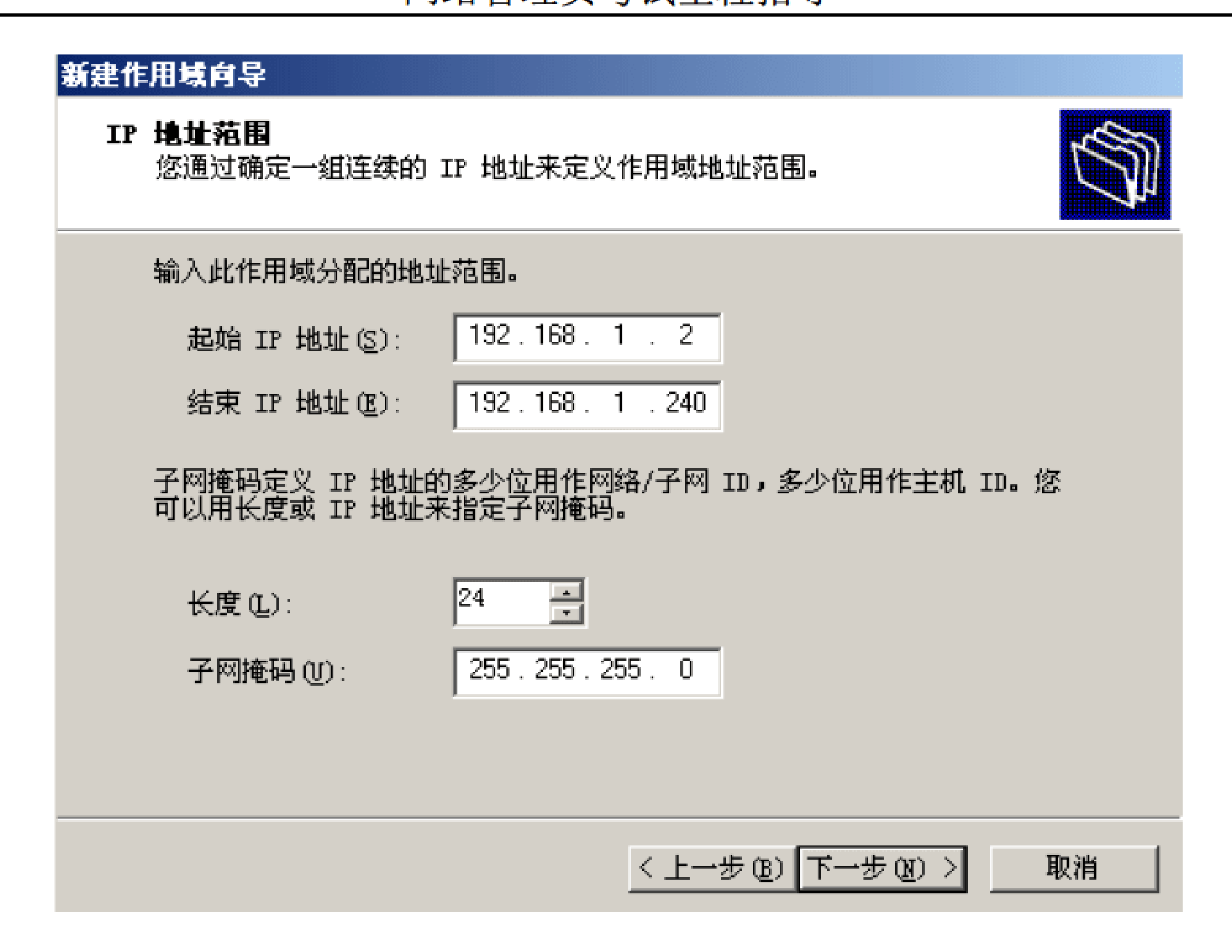


图 12-29　IP 地址范围

图 12-29 所示的对话框中可指定作用域的地址范围及子网掩码。DHCP 管理器会为用户提供一个适用于大多数网络的默认子网掩码。如果该默认值不正确，可以在“长度”或“子网掩码”文本框中输入正确的值。单击“下一步”按钮，弹出“添加排除”对话框，如图 12-30 所示。

图 12-30　添加排除

图 12-30 所示的对话框中可定义服务器不分配的 IP 地址范围。排除范围应包括所有

手工分配给其他 DHCP 服务器、非 DHCP 客户机等。单击“下一步”按钮，进入“租约期限”对话框，如图 12-31 所示。

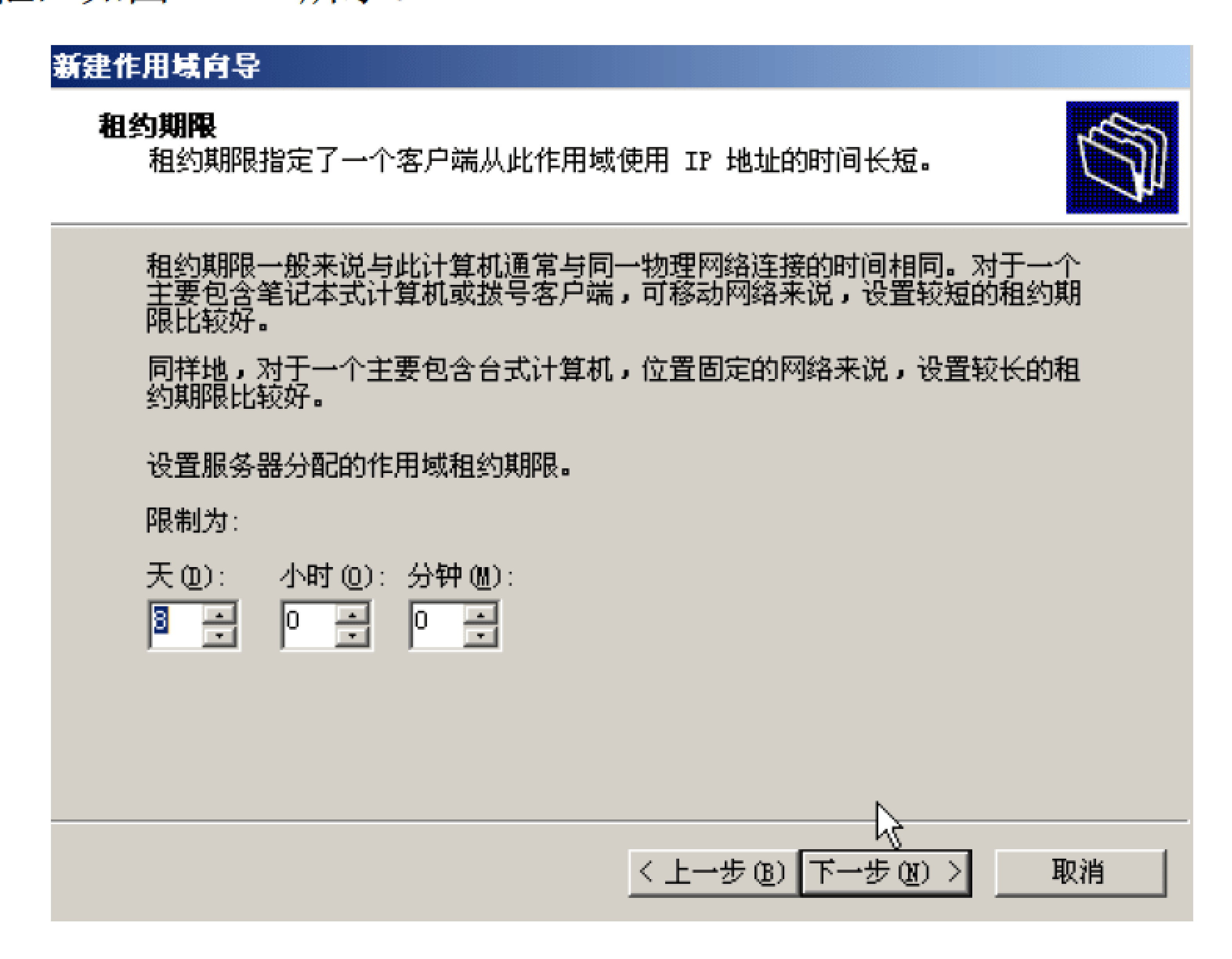


图 12-31　租约期限

在图 12-31 中，租约期限指定了客户机使用 DHCP 服务器所分配的 IP 地址的时间。要想让网络客户使用作用域，必须配置最常用的 DHCP 选项，这些选项包括网关、DNS 服务器和 WINS 设置等。在“路由器（默认网关）”对话框，如图 12-32 所示。

新建作用域向导
路由器(默认网关)
您可为指定此作用域要分配的路由器或默认网关。
要添加客户端使用的路由器的 IP 地址，请在下面输入地址。
IP 地址(P):
添加(D)
192.168.1.254
删除(R)
上移(U)
下移(O)
< 上一步(B)
下一步(N) >
取消

图 12-32　路由器（默认网关）

单击“下一步”按钮，弹出“激活作用域”对话框，如图 12-33 所示。



图 12-33 激活作用域

在图 12-33 中，选择“是，我想现在激活此作用域”按钮。最后单击“完成”按钮，关闭“新建作用域向导”对话框，在 DHCP 控制台上就列出了刚才所创建的作用域，如图 12-34 所示。

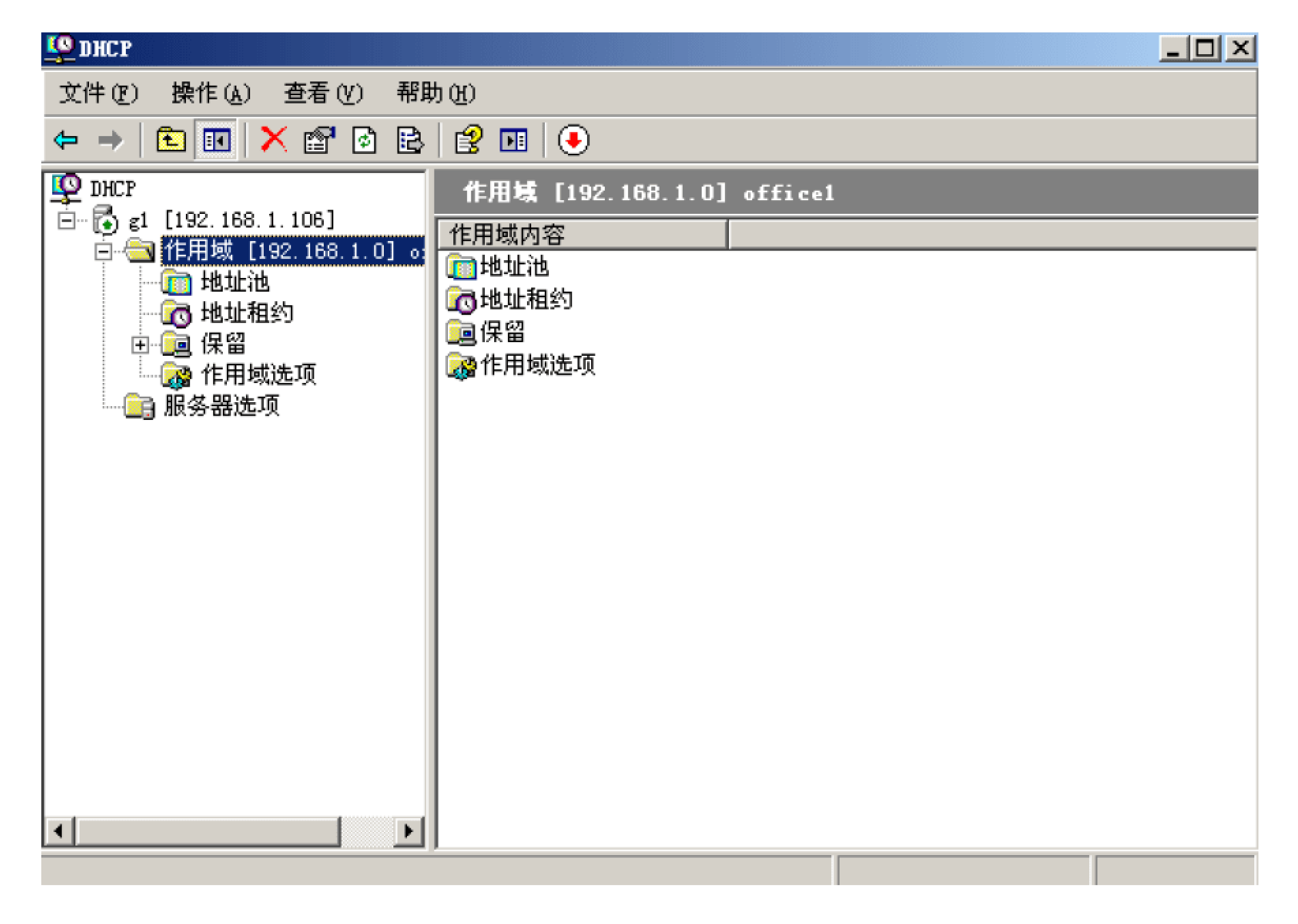


图 12-34 新建的作用域

2．DHCP 中继代理

Windows 服务器系统内置的中继代理功能，完全可以将原先的 DHCP 服务器利用起来，分别为多个不同子网提供 IP 地址分配服务。下面，以一台 DHCP 服务器同时为两个子网提供地址分配服务为例，来详细介绍一下如何启用 DHCP 中继代理程序，协助不同子网中的工作站完成跨子网申请 IP 地址的任务。

1）配置虚拟路由

在启用 DHCP 中继代理功能之前，需要先将工作站配置成一个虚拟的路由器，以便利用该路由器将局域网中的两个不同子网连接起来。Windows 系统在默认状态下没有启用路由和远程访问服务，因此我们必须先用手工方法来安装配置好该服务。

依次打开系统控制面板窗口中的“管理工具”图标，再双击“路由和远程访问”项目，打开如图 12-35 所示的路由和远程访问界面。



图 12-35　路由和远程访问界面

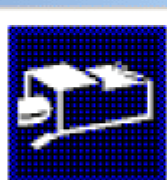
在图 12-35 中，右击本地计算机图标，从弹出的右键菜单中执行“配置并启用路由和远程访问”命令，打开路由和远程访问服务器安装向导窗口，单击该窗口中的“下一步”按钮，进入到如图 12-36 所示的向导配置界面。

在图 12-36 中，选中该界面中的“自定义配置”选项，再单击“下一步”按钮，在其后出现的向导窗口中选中“LAN 路由”复选项，如图 12-37 所示。

路由和远程访问服务器安装向导

配置

您可以启用下列服务的任意组合，或者您可以自定义此服务器。



○ 远程访问(拨号或 VPN)(R)

允许远程客户端通过拨号或安全的虚拟专用网络(VPN) Internet 连接来连接到此服务器。

○ 网络地址转换(NAT)(E)

允许内部客户端使用一个公共 IP 地址连接到 Internet。

○ 虚拟专用网络(VPN)访问和 NAT(V)

允许远程客户端通过 Internet 连接到此服务器，本地客户端使用一个单一的公共 IP 地址连接到 Internet。

○ 两个专用网络之间的安全连接(S)

将此网络连接到一个远程网络，例如一个分支办公室。

◉ 自定义配置(C)

选择在路由和远程访问中的任何可用功能的组合。

有关这些选项的更多信息，请参阅路由和远程访问帮助。

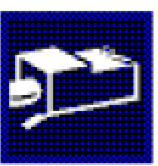
< 上一步(B) 下一步(N) > 取消

图 12-36 向导配置界面

路由和远程访问服务器安装向导

自定义配置

关闭此向导后，您可以在路由和远程访问控制台中配置选择的服务。



选择您想在此服务器上启用的服务。

- [ ] VPN 访问(V)
- [ ] 拨号访问(D)
- [ ] 请求拨号连接(由分支办公室路由使用)(E)
- [ ] NAT 和基本防火墙(A)
- [x] LAN 路由(L)

< 上一步(B) 下一步(N) > 取消

图 12-37 向导窗口

最后单击【完成】退出路由和远程访问服务器安装向导窗口。

2）启用 DHCP 中继代理

所谓“中继代理”，其实就是为处于不同子网中的工作站与服务器之间中转传输 BOOTP/DHCP 消息的一种特殊程序，为了实现 DHCP 中继代理功能，需要配置一个 DHCP 中继代理服务器，位于同一子网中的工作站以广播方式申请IP 地址时，DHCP 中继代理服务器就会自动将 IP 地址申请信息中转传输到位于另外一个子网中的 DHCP 服务器，DHCP 服务器再将 IP 地址应答信息通过中继代理服务器转发给指定的工作站，从而协助工作站完成跨子网申请 IP 地址服务。系统在默认状态下并没有安装 DHCP 中继代理程序，因此须先将 DHCP 中继代理程序安装好。

首先，进入图 12-35 所示的路由和远程访问界面，然后逐一展开该界面左侧区域的“本地计算机”→“IP 路由选择”→“常规”选项。再单击“常规”选项，从快捷菜单中选择“新增路由协议”命令，打开如图 12-38 所示的设置对话框。

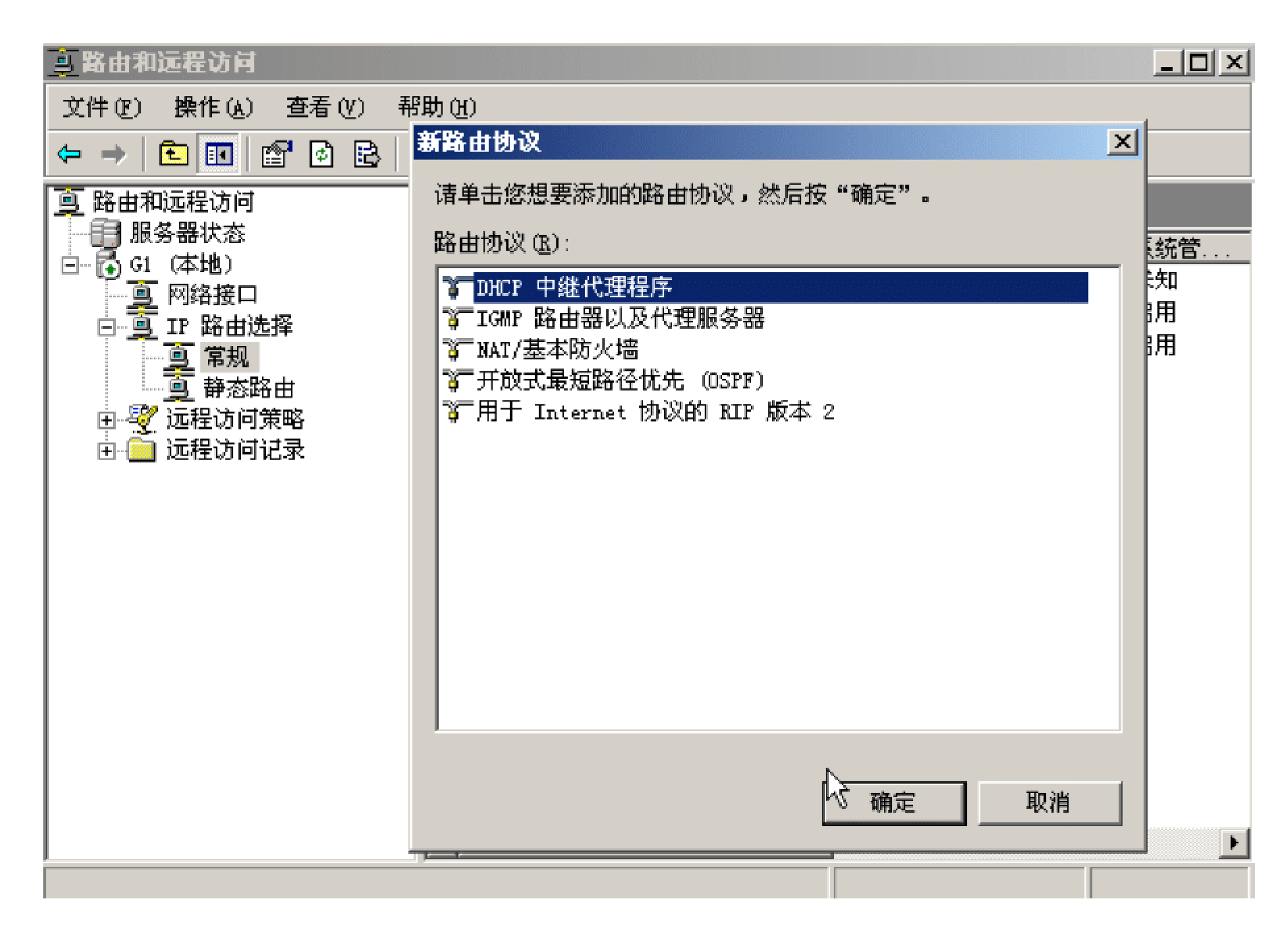


图 12-38　新路由协议

在图 12-38 中，选中“路由协议”列表框中的“DHCP 中继代理程序”选项，再单击“确定”按钮结束 DHCP 中继代理程序的安装操作。

指定 DHCP 服务器，右键单击前面已经安装好的“DHCP 中继代理程序”项目，执行“属性”命令，打开如图 12-39 所示的 DHCP 中继代理程序属性设置窗口；在“常规”标签中，将位于另外一子网的 DHCP 服务器 IP 地址准确地填写在此处的“服务器地址”

文本框中，例如 DHCP 服务器 IP 地址是“192.168.1.55”，再单击一下“添加”按钮，完成 DHCP 服务器的指定工作；要是局域网中包含有多个 DHCP 服务器时，可以分别将这些 DHCP 服务器的 IP 地址添加到这里。

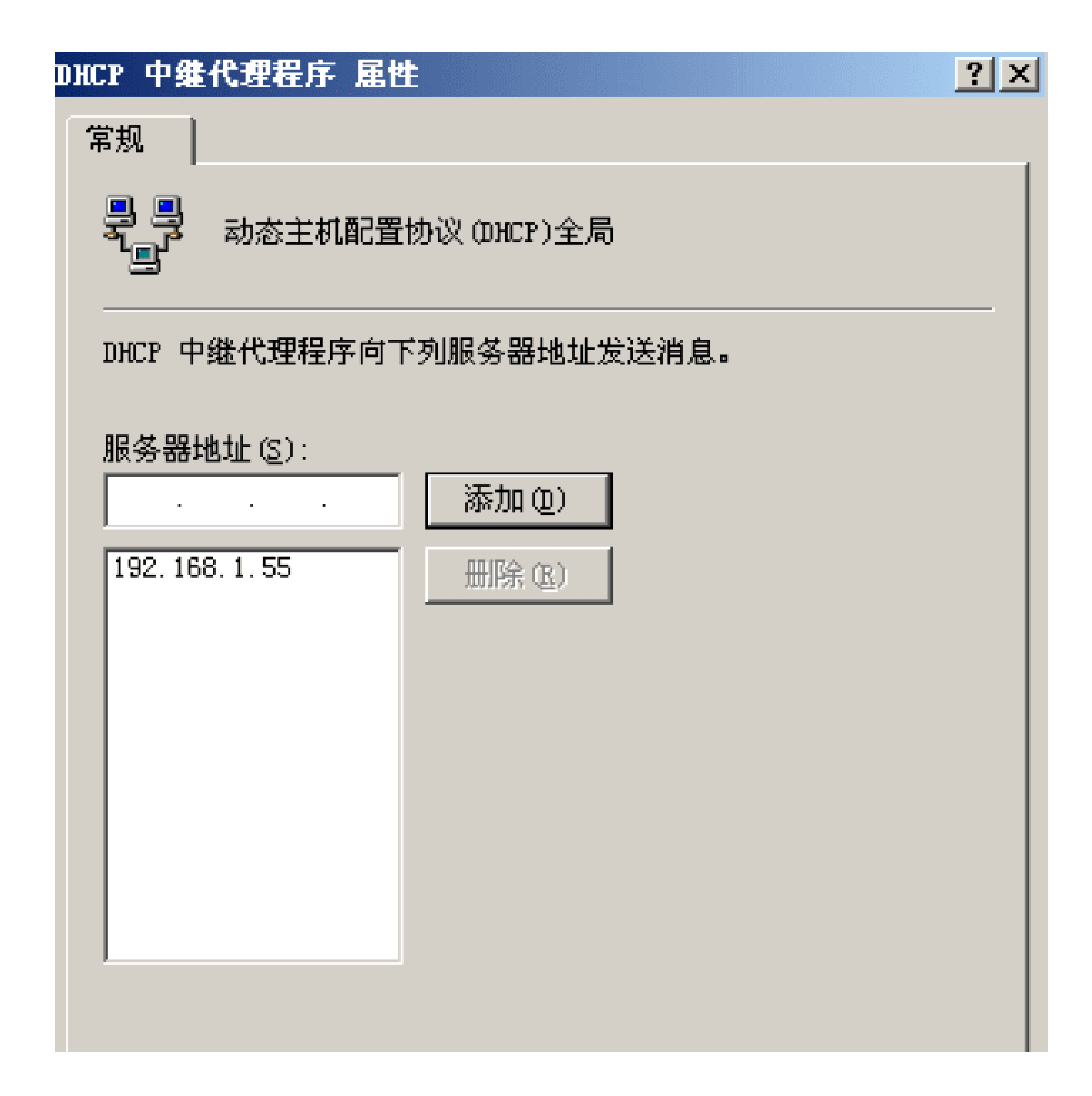


图 12-39 中继代理程序

完成好上面的各项工作后，DHCP 中继代理程序现在还不能立刻发挥作用，我们还必须对其访问接口进行一下合适配置。在配置 DHCP 中继代理程序的访问接口时，我们还需要先进入路由和远程访问界面。

首先，展开该界面左侧区域的“本地计算机”→“IP 路由选择”→“DHCP 中继代理程序”选项，再用鼠标右键单击“DHCP 中继代理程序”选项，从其后弹出的快捷菜单中选择“新增接口”命令，打开中继代理程序的新接口设置对话框，选中能够与位于另外一子网中的 DHCP 服务器直接通信的那个接口选项（通常该接口就是连接另外一个子网的网卡）。选好目标接口之后，单击“确定”按钮，弹出如图 12-40 所示的 DHCP 中继站属性设置对话框。

将图 12-40 中的“中继 DHCP 数据包”复选项选中，同时设置好“跃点计数阈值”以及“启动阈值”这两个参数（一般保持默认数值），最后单击“确定”按钮，这样 DHCP 中继代理功能就能开始发挥作用了。

到了这里，DHCP 中继代理程序就能实现跨子网地址申请中转服务了；以后，和 DHCP 中继代理服务器位于相同子网的工作站，就能通过 DHCP 中继代理程序来向位于另外一个子网的 DHCP 服务器申请动态 IP 地址了。

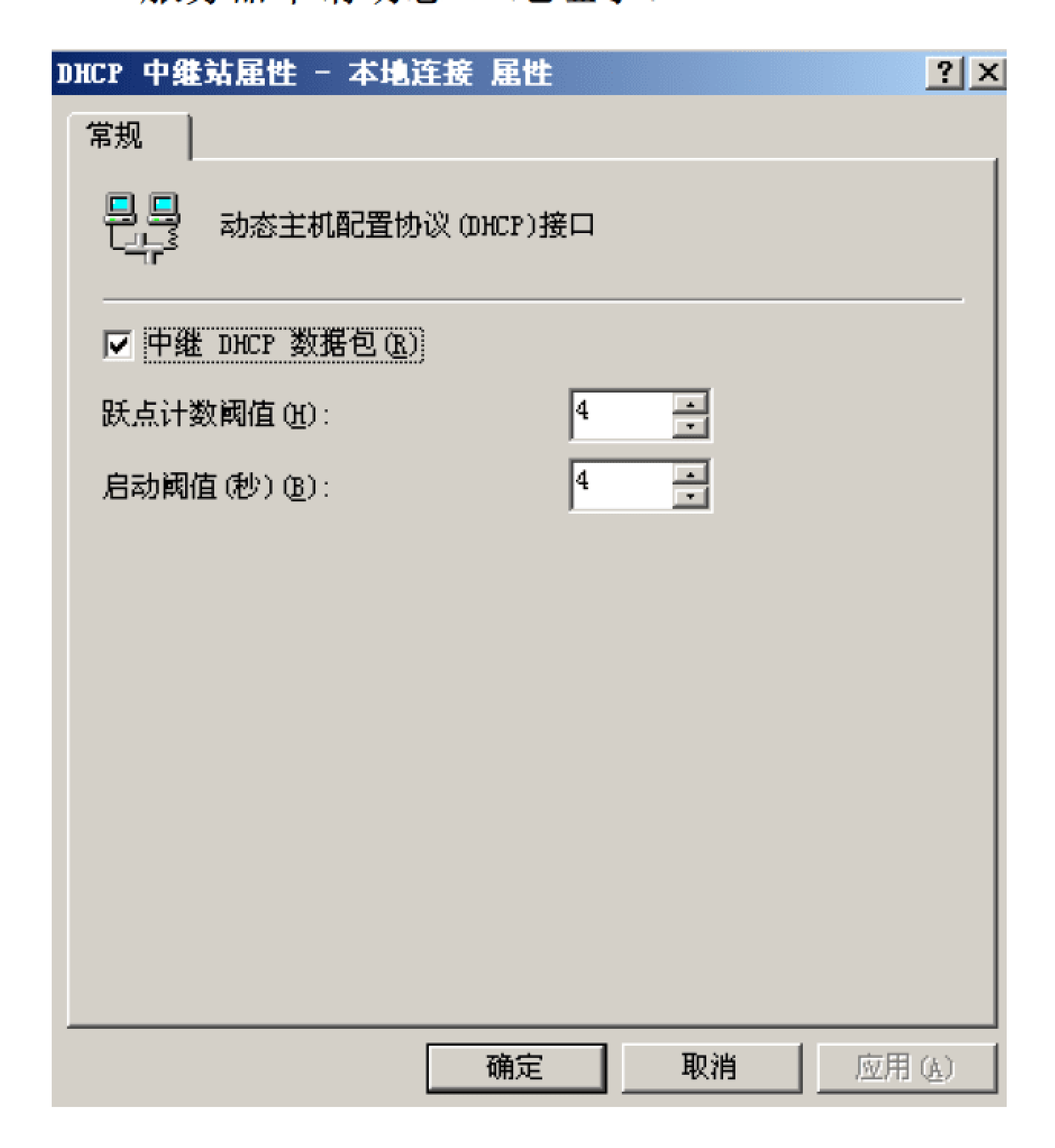


图 12-40　中继站属性设置

3．DHCP 客户机设置

为了使客户端计算机能够自动获得 IP 地址，除了 DHCP 服务器正常工作外，还需要将客户端计算机配置成自动获得 IP 地址的方式。以 Windows XP 系统为例对客户端计算机进行了配置，具体方法如下：

（1）在桌面上右击“网上邻居”图标，选择“属性”命令。

（2）在打开的“网络连接”窗口中，双击“本地连接”图标，选择“属性”命令。接着双击“Internet 协议（TCP/IP）属性”选项，选中“自动获得 IP 地址”，并单击“确定”按钮即可，如图 12-41 所示。

12.5.3　Linux 平台下 DHCP 服务配置

在 Linux 下配置 DHCP，主要工作是对相关文件进行解析。

1．DHCP 启动与停止

可以使用以下命令来启动、停止和重启 dhcpd 服务器程序：



图 12-41　设置 DHCP 客户端

```
[root@lib1root]#servicedhcpd[start|stop|restart]
```

或

```
[root@lib1root]#etc/init.d/dhcpd[start|stop|restart]
```

其中 start、stop、restart 为任选参数，分别表示启动、停止和重启。执行以上命令启动后，dhcpd 默认是启动在 eth0 上，如果 dhcpd 上的服务器还有另外一块网卡 eth1，想在 eth1 上启动 dhcpd，就键入：

```
[root@lib1root]#/usr/sbin/dhcpdeth1
```

2．配置文件解析

DHCP 默认的配置文件是/etc/dhcpd.conf，它是个递归下降格式的配置文件，有点像 C 的源程序风格，由参数和声明两大类语句构成，参数类语句主要告诉 dhcpd 网络参数，如租约的时间、网关、DNS 等，而声明语句则是描述网络的拓扑，用来表明网络上的客户、要提供给客户的 IP 地址、提供一个参数组给一组声明等。参数类又分标准参数语句和选项类语句，这里给出 dhcpd.conf 配置文件中最常用和最重要的语句。

1）参数类与选项类语句

DHCP 配置语句如表 12-6 所示。

表 12-6　DCHP 配置语句

类型	语句格式	功能与参数描述
标准参数类语句	ddns-update-style*type*	动态 DNS 解析方式，可选参数分别为：ad-hoc、interim、none
	default-lease-time*time*	指定默认租约时间，这里的 time 是以秒为单位的。如果 DHCP 客户在请求一个租约但没有指定租约的失效时间，租约时间就是默认租约时间
	max-lease-time*time*	最大的租约时间。如果 DHCP 在请求租约时间内有发出特定的租约失效时间的请求，则用最大租约时间
	Hardware　hardware-type hardware-address	指明物理硬件接口类型和硬件地址。硬件地址由 6 个 8 位组构成，每个 8 位组以“：”隔开。如 00：00：E8：1B：54：97
	server-name"*name*"	用于告之客户端所连接服务器的名字
	fixed-address*address*[,*address*...]	用于指定一个或多个 IP 地址给一个 DHCP 客户，只能出现在 host 声明里
选项类语句	optionsubnet-mask*mask*	DHCP 服务配置子网掩码选项，服务开启后可应用于所有客户端
	optionbroadcast-address*IP 地址*	DHCP 服务配置广播地址选项，服务开启后可应用于所有客户端
	optionrouters*IP 地址*	同上，DHCP 服务配置网关（路由）地址选项，可设多个
	optiondomain-name-servers *IP 地址*	DHCP 服务配置 DNS 服务器地址，可应用于所有客户端，可多个
	optiondomain-name"*csai.cn*"	DHCP 服务配置域名服务，可应用于所有客户端
	optionhost-name*string*	给客户指定主机名，string 是个字符串

2）声明类语句

```
share-network 语句
shared-networkname{
[参数]
[声明]
}
```

share-network 用于告诉 DHCP 服务器某些 IP 子网其实是共享同一个物理网络。任何一个在共享物理网络里的子网都必须声明在 share-network 语句里。当属于其子网里的客户启动时，将获得在 share-network 语句里指定参数，除非这些参数被 subnet 或 host 里的参数覆盖。用 share-network 是一种权宜之计，例如某公司用 B 类网络 145.252.0.0，公司里的部门 A 被划在子网 145.252.1.0 里，子网掩码为 255.255.255.0，这里子网号为 8

位，主机号也为 8 位，但如果部门 A 急速增长，超过了 254 个节点，而物理网络还来不及增加，就要在原来这个物理网络上加两个 8 位掩码的子网，而这两个子网其实是在同一个物理网络上。

share-network 语句可以如下：

```
shared-network share1{                #share1 这里是共享网络名
subnet 145.252.1.0 netmask255.255.255.0{
range 145.252.1.10 145.252.1.253;
}
subnet 145.252.2.0 netmask 255.255.255.0{
range 145.252.2.10 145.252.1.253;
}
}
subnet 语句
subnet subnet-number net mask netmask{
[参数]
[声明]
}
```

subnet 语句用于提供足够的信息来阐明一个 IP 地址是否属于该子网。也可以提供指定的子网参数和指明那些属于该子网的 IP 地址可以动态分配给客户，这些 IP 地址必须在 range 声明里指定。subnet-number 可以是个 IP 地址或能被解析到这个子网的子网号的域名。netmask 可以是个 IP 地址或能被解析到这个子网的掩码的域名。例如：

```
subnet 192.168.0.1 netmask 255.255.255.0{ #子网声明和掩码
range 192.168.1.10 192.168.1.100;         #地址段范围
range 192.168.1.150 192.168.1.200;        #地址段范围
}
```

这段配置文件将允许 DHCP 服务器分配两段地址范围给 DHCP 客户，192.168.1.10-100 和 192.168.1.150-200。服务器发送下面的参数给 DHCP 客户机：子网掩码是 255.255.255.0，广播地址是 192.168.1.255，默认网关是 192.168.1.1，DNS 是 192.168.1.1。

```
range 语句
range[dynamic-bootp]low-address[high-address];
```

对于任何一个有动态分配 IP 地址的 subnet 语句里，至少要有一个 range 语句，用来指明要分配的 IP 地址的范围。如果只指定一个要分配的 IP 地址，高地址部分可以省略。

```
host 语句
```

host 语句的作用是为特定的客户机提供网络信息。

```
host host name{
[参数]
[声明]
}
```

例如，如果为一台名为 WebServer 主机指定固定的 IP 地址，可以在 dhcpd.conf 文件添加如下语句：

```
host Web Server{
hardwareethernet08:00:00:4c:58:23;   #指定主机上网卡接口及硬件地址
  fixed-address192.168.1.210;         #固定 IP，这两条命令参见参数类语句
}
```

group 语句：组语句给一组声明提供参数。

```
group{
[参数]
[声明]
}
allow 和 deny 语句
```

allow 和 deny 语句用来控制 dhcpd 对客户的请求。它有两个可选关键字，即 unknown-clients 关键字和 bootp 关键字。

```
allow[unknown-clients|bootp];
deny[unknown-clients|bootp];
```

allowunknown-clients 允许 dhcpd 可以动态分配 IP 给未知的客户，而 denyunknown-clients 则不允许。默认是允许的。bootp 关键字指明 dhcpd 是否响应 bootp 查询，默认是允许的。

3．dhcpd.leases 文件解析

dhcpd.leases 是 DHCP 客户租约的数据库文件，默认目录在/var/state/dhcp/，文件包含租约声明，每次一个租约被获取、更新或释放，它的新值就被记录到文件的末尾。

```
leaseip-address{statements...}
```

每个记录包含一个提供给客户的 IP 地址，在花括号里的语句包含一些租约信息。具体的租约信息因客户发出不同的 DHCP 请求而稍有差别。

例如，在主机 CSAI_USER 获得租约后，dhcpd 会在 dhcp.leases 里建一条记录：

```
lease192.168.1.100{
starts12000/05/1513:36:42;
```

```
ends12000/05/1521:36:42;
hardwareethernet00:00:21:4e:3f:58;
uid01:00:00:21:4e:3f:58;
client-hostname"CSAI_USER";
}
```

要注意的是 dhcpd.leases 的时间记录采用 GMT 时间，而不是本地时区的时间（GMT+8:00）。

以上就是 dhcpd 常用配置，在实际应用 DHCP 还要考虑 IP 分配的一些策略问题，同时要保证网络的健壮性，必须至少要有两台 DHCP 服务器一起工作，如果一台出了故障，另一台可以继续为 DHCP 客户服务。然而目前 DHCP 协议里并没有能让两台 DHCP 服务器协同工作的机制，不能保证分配的地址的唯一性，所以这两台 DHCP 服务器里的可分配地址空间必须进行调整，不能有交叉重复的 IP 地址。

12.6 Samba 服务

Samba（smb）是为 Linux-Windows 互连共享资源而设计的程序。主要用于不同操作平台之间共享文件和打印机。它也一样用于 Linux 和 Linux 之间的共享文件，不过对于 Linux 和 Linux 之间共享文件有更好的网络文件系统 NFS。Samba 有两个服务程序：smb 和 nmb，smb 是 Samba 的主要启动服务，让其他机器能知道此机器共享了什么；nmb 是把这台 Linux 机器所共享的工作组及在此工作组下的 NetbiosName 解析出来，如果不打开 nmb 服务器的话，只能通过 IP 来访问。

12.6.1 Samba 基础配置

Samba 基础配置包括 Samba 服务的启动，Smb.conf 文件配置等等。

1．Samba 启动

用以下命令可以直接启动、关闭与重启 Samba 服务：

[root@lib1root]#servicesmb[start|stop|restart] 或 [root@lib1root]#etc/init.d/smb[start|stop|restart]

其中 start、stop、restart 为任选参数，分别表示启动、停止和重启。

2．Samba 服务的配置文件

Samba 服务的配置文件是 etc/samba /smb.conf。此文件中用“＃”和“;”表示注释语句。smb.conf 文件有三个主要部分：

（1）全局参数字段（gobal)：主机共享时的整体设置。

（2）目录共享字段（homes)：定义一般参数，如建立共享文件目录等。

（3）打印机共享字段（printers)：打印机的配置和共享。

下面对 smb.conf 文件中的主要设置项逐一解释说明：

```
[global]
```

workgroup=CSAIGROUP#此参数设置服务器所要加入工作组名称，系统默认为 MYGROUP。

netbiosname=LinuxSir#此参数在配置文件中未列出，需手动添加，用于设置显示在“网上邻居”中的主机名。

serverstring=LinuxSamba#此参数描述 Samba 服务器的一些信息，这些注释信息会显示在“网上邻居”中。

```
security=[user|share|Server|Domain]
```

#此可选参数用于设置 Samba 服务器的安全模式。

#user 模式：当主机访问 Samba 服务器时，需要输入用户名与密码，该用户必须属于服务器注册用户。

#share 模式：当主机访问 Samba 服务器时，不需要输入用户名与密码，即对所有主机或用户共享。

#Server 模式：需要输入用户名与密码，验证用户信息由另一服务器负责，而非 Samba 服务器。

#Domain 模式：与 Server 模式类似，使用域中的服务器来验证用户信息。

```
Hostallow=192.168.1.192.168.2.127.
```

#此参数设置哪些 IP 允许访问该服务器，本例中允许的网段分别是：192.168.1.0，192.168.2.0，127.0.0.0。

dnsproxy=[yes|no]#此参数设置 Samba 服务器是否作为 DNS 服务的代理解析。

[homes]

comment=HomeDirectories#对共享资源的注释说明。

browseable=[yes|no]#设置是否允许浏览文件或目录。

writable=[yes|no]#设置是否允许往目录里写入文件。

Validusers=%S#设置可访问的用户，系统会自动将%S 转换成登录账号。

createmask=0664

#createmask 是用户创建文件时的权限掩码；对用户来可读可写，对用户组可读可写，对其他用户可读。

```
directorymask=0775
```

#directorymask 是用来设置用户创建目录时的权限掩码，意思是对于用户和用户组

可读可写，对其他用户可读可执行。

[printers]
comment=allprinters
path=/var/spool/samba#设置打印机队列位置。
browseable=[yes|no]#设置是否允许浏览打印机。
Guestok=[yes|no]#访问打印机时是否需要密码。
writable=[yes|no]#共享打印机必须设置为 NO。

12.6.2 Samba 用户管理

Samba 用户管理包括导入系统用户和添加新用户。

1．导入系统用户

Samba 服务的用户必须保证是 Linux 系统已存在的用户，因此在添加 Samba 用户前，可以使用如下命令将系统用户导入到 Samba 服务中：

```
[root@lib1smaba]#cat/ect/passwd|mksmbpasswd.sh>/ect/samba/smbpasswd
```

2．添加新用户

可以为 Samba 服务单个添加新用户，添加的新用户必须是已存在的系统用户。先按照下面命令建立系统用户：

```
[root@lib1smaba]#useraddcsaiuser1
```

再将其添加到 Samba 服务用户中：

```
[root@lib1smaba]#sambaddusercsaiuser1:csaiuser1
```

12.6.3 Samba 共享配置

下面给出一个具体实例：假设在服务器上设置一个共享目录 public，不需要用户名与密码就可以为所有用户共享访问；并为用户 csaiuser1 创建个人目录/usr/csaiuser1_dir，只有 csaiuser1 可以访问。

1．创建目录及共享资源并设置权限

在/home 目录下创建 public 目录，设置权限为可读写。在/usr 目录下创建 csaiuser1_dir 目录，设置权限为可读写。

```
[root@lib1home]#mkdirpublic
[root@lib1home]#chmod777public
[root@lib1usr]#mkdircsaiuser1_dir
[root@lib1home]#chmod777csaiuser1_dir
```

2．修改 smb.conf 文件

在 sharedefinitions 区域添加如下内容：

```
[public]
comment=publicdirectories
browseable=yes
path=/home/public
writable=yes
public=yes
[csaiuser1_dir]
comment=user1 directories
path=/usr/csaiuser1_dir
validusers=csaiuser1
writable=yes
public=no
```

文件修改后，必须重启 Smaba 服务器才能生效。

12.6.4　Linux 访问 Windows

Linux 主机访问 Windows 主机资源时，可以使用两个命令：smbclient 或 smbmount，下面以 Linux 主机 Lib1（192.168.0.1）配置为 Smaba 服务器，访问 Windows 主机 Lib2（192.168.0.2）上的共享资源 D:/Win_share 目录为例来讲解这两个命令。

1．smbclient 命令

该命令既可以查看并访问 Windows 主机提供的共享资源，也可以查看本机（Smaba 服务器）提供的共享资源。

（1）查看本机提供的资源时，命令如下：

```
[root@lib1smaba]#smbclient-LLocalhost
```

（2）查看 Windows 主机提供的资源时，命令如下：

```
[root@lib1smaba]#smbclient-Llib2-Uadministrator
```

（3）查看 Windows 主机提供的资源时，命令如下：

```
[root@lib1smaba]#smbclient//lib2/win_share-Uadministrator
smb:\>
```

在 smb:\>提示符后，可以使用如 FTP 一样的命令方法来使用 smbclient。如“dir：”显示当前共享目录信息；“get：”下载所需要的文件。

2．smbmount 命令

该命令可将共享的 Windows 目录直接挂载到 Linux 系统的本地目录（类似于磁盘映射）。这样可以像访问本机目录一样，来操作挂载目录，从而访问 Windows 主机资源。

```
[root@lib1smaba]#mkdir/mnt/samba
[root@lib1smaba]#smbmount//lib2/win_share/mnt/sambausername=csaiuser1
```

卸载已挂载目录可以使用 umount 命令：

```
[root@lib1smaba] #umount/mnt/samba
```

12.6.5 Windows 访问 Linux

打开 Windows 的 IE，用 IP 地址的访问方式就能访问了，格式为\\192.168.0.1 类型。也可以通过网上邻居等传统 Windows 访问方式访问 Linux 资源。

12.7 例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 8 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

某主机使用代理服务器接入 Internet，应该在其 IE 浏览器的__（1）__对话框中进行配置。

（1）A．“工具”→“Internet 选项…”→“常规”

B．“工具”→“Internet 选项…”→“连接”→“局域网设置”

C．“工具”→“Internet 选项…”→“安全”

D．“工具”→“Internet 选项…”→“程序”→“重置 Web 设置”

例题 1 分析

要使用代理服务器接入 Internet，应该在 IE 浏览器的“工具”→“Internet 选项…”→“连接”→“局域网设置”中进行配置代理服务器的 IP 地址及端口号。

例题 1 答案

（1）B

例题 2

在 Windows 操作系统中，可以通过__（2）__命令查看 DHCP 服务器分配给本机的 IP 地址。

（2）A．ipconfig/all　　B．ipconfig/find

C．ipconfig/get　　D．ipconfig/see

例题 2 分析

如果计算机及其所在的局域网使用了动态主机配置协议（Dynamic Host Configuration Protocol，DHCP），这时，IPConfig 命令可以让你了解计算机是否成功地租用到一个 IP 地址，如果租用到则可以了解它目前分配到的是什么地址。了解计算机当前的 IP 地址、子网掩码和缺省网关，实际上是进行测试和故障分析的必要网络配置信息。该命令最常用的选项如下：

（1）ipconfig：当使用 ipconfig 时不带任何参数选项，那么它为每个已经配置了的接口显示 IP 地址、子网掩码和缺省网关值。

（2）ipconfig /all：当使用 all 选项时，ipconfig 能为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息（如 IP 地址等），并且显示内置于本地网卡中的物理地址（MAC）。如果 IP 地址是从 DHCP 服务器租用的，ipconfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。

（3）ipconfig /release 和 ipconfig /renew：这是两个附加选项，只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。如果你输入 ipconfig /release，那么所有接口的租用 IP 地址便重新交付给 DHCP 服务器（归还 IP 地址）。如果你输入 ipconfig /renew，那么本地计算机便设法与 DHCP 服务器取得联系，并租用一个 IP 地址。

例题 2 答案

（2）A

例题 3

下面能实现 NAT 的是__（3）__。

（3）A．DNS 服务器　　B．代理服务器
　　C．FTP 服务器　　D．Web 服务器

例题 3 分析

NAT（网络地址转换），是通过将私用网络地址（如企业内部网 Intranet）转换为公用地址（如因特网 Internet），从而对外隐藏了内部管理的 IP 地址。这样，通过在内部使用非注册的 IP 地址，并将它们转换为一小部分外部通用的公网 IP 地址，从而减少了 IP 地址注册的费用及节省了越来越缺乏的地址空间。同时，这也隐藏了内部网络结构，从而降低了内部网络受到攻击的风险。

NAT 功能通常被集成到路由器、防火墙、单独的 NAT 设备中，当然，现在比较流行的操作系统或其他软件（主要是代理软件，如 WINROUTE，安装在主机上，形式代理服务器），大多也有着 NAT 的功能。

例题 3 答案

（3）B

例题 4

Windows Server 2003 操作系统中，IIS 6.0 不提供下列__（4）__服务。

（4）A．Web　　B．SMTP　　C．POP3　　D．FTP

例题 4 分析

IIS 是 Internet Information Server 的缩写，它是微软公司主推的服务器，目前普遍的版本是 Windows 2003 里面包含的 IIS 6.0，IIS 支持 HTTP（Hypertext Transfer Protocol，超文本传输协议）、FTP（Fele Transfer Protocol，文件传输协议）以及 SMTP 协议。

例题 4 答案

（4）C

例题 5

Linux 操作系统中，网络管理员可以通过修改＿（5）＿文件对 Web 服务器的端口进行配置。

（5）A．/etc/inetd.conf　　B．/etc/lilo.conf

C．/etc/httpd/conf/ httpd.conf　　D．/etc/httpd/conf/access.conf

例题 5 分析

Apache 服务器的配置文件存放于/etc/httpd/conf/目录下，其主配置文件为 httpd.conf，所有的配置信息均存放在该文件中。Apache 服务端口，默认值为 80（port 80），如果希望 Apache 服务器在其他特殊的端口服务，则需要修改参数。

例题 5 答案

（5）C

例题 6

阅读以下关于 Linux 系统中域名系统（DNS）的说明，回答问题 1 至问题 4。

【说明】

DNS 是一种 TCP/IP 的标准服务，负责 IP 地址和域名之间的转换。在 Linux 系统中，DNS 可以由 BIND（Berkeley Internet Name Domain）软件来实现。

【问题 1】

请在（1）～（4）空白处填写适当的内容。

DNS 服务器可以管理一个域，也可以管理多个域。域名服务器可以分为转发域名服务器、缓存域名服务器、＿（1）＿和＿（2）＿等类型。将域名转换为IP 地址的过程称为＿（3）＿，将 IP 地址转换为域名的过程称为＿（4）＿。

【问题 2】

请选择适当的内容填写在（5）、（6）空白处。

管理员可以在命令行终端下，通过＿（5）＿命令启动 DNS 服务；通过＿（6）＿命令停止 DNS 服务。

（5）、（6）备选答案：

A．/etc/init.d/named start　　B．/etc/init.d/dns up

C．/etc/init.d/named stop　　D．/etc/init.d/dns down

【问题 3】

请在（7）～（9）处填写恰当的内容。

在 Linux 系统中配置域名服务器，该服务器上文件 named.conf 的部分内容如下：

```
options {
        directory '/var/named';
    };
    zone '.' {
        type hint;
        file 'named.ca';
    }
    zone 'localhost' IN {
        file "localhost.zone"
        allow-update{none;};
    };
    zone '0.0.127.in-addr.arpa'{
        type master;
        file 'named.local';
    };
    zone 'test.com'{
        type (__(7)__) ;
        file 'test.com';
    };
    zone '40.35.222.in-addr.arpa'{
        type master;
        file '40.35.222';
    };
    include "/etc/rndc.key";
```

填写文件中空（7）处缺省的内容。

该服务器是域 test.com 的主域名服务器，该域对应的网络地址是＿（8）＿，正向域名转换数据文件存放在＿（9）＿目录中。

【问题 4】

希赛公司内部网的 DNS 服务器发生故障，如不改变客户机原有设置，该网用户是否可以访问网络上的资源？如果可以，需要什么条件？如果不可以，请说明原因。

例题 6 分析

【问题 1】

域名服务器可以分为：转发域名服务器、缓存域名服务器、主域名服务器、辅助域名服务器。将域名转换为 IP 地址的过程称为正向解析，将 IP 地址转换为域名的过程称

为反向解析。

【问题 2】

管理员可以在命令行终端下，通过/etc/init.d/named start 命令启动 DNS 服务；通过/etc/init.d/named stop 命令停止 DNS 服务。

【问题 3】

题目给出该服务器的域 test.com 的主域名服务器因此（7）填写 master，表明为主域名服务器。

由配置文件中的“zone '40.35.222.in-addr.arpa'{ ”语句可以知道 test.com 对应的 IP 地址为 222.35.40.0。

由配置文件中的“directory '/var/named'; ”可以知道正向域名转换数据文件存放在/var/named 目录中。

【问题 4】

如果仅仅是 DNS 服务器发生故障，那么仍然可以上网的。应该回答“可以”。只需要知道被访问端的 IP 地址即可。

例题 6 答案

【问题 1】

（1）主域名服务器 （2）辅助域名服务器 （3）正向解析 （4）反向解析

【问题 2】

（5）A （6）C

【问题 3】

（7）master （8）222.35.40.0 （9）可以，只需要知道被访问端的 IP 地址即可。

例题 7

某内部局域网连接方式如图 12-42 所示，客户机通过代理服务器访问 Internet。代理服务器的公网 IP 为 61.194.101.35/24。

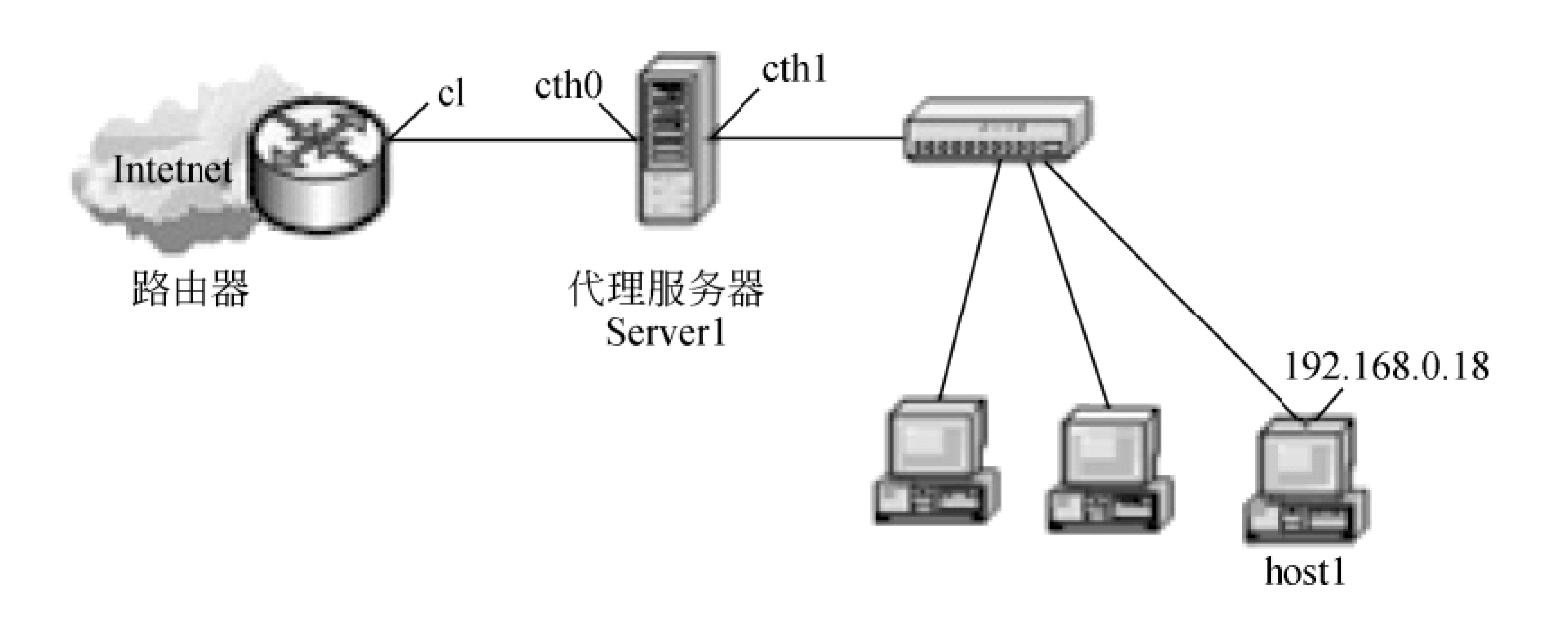


图 12-42 某局域网连接方式

在主机 host1 的 Windows 命令行窗口输入 tracert www.abc.com 命令后，测试到目的站点所经过的连接情况如图 12-43 所示。

```
C:\Documents and Settings\User>tracert www.abc.com

Tracing route to www.abc.com [210.200.3.143]
over a maximum of 30 hops:

  1     <1 ms    <1 ms    <1 ms  192.168.1.1
  2   1580 ms    63 ms    11 ms  61.194.101.254
  3      4 ms     1 ms     1 ms  202.200.29.141
  4      1 ms     1 ms     1 ms  202.200.29.9
  5     <1 ms    <1 ms    <1 ms  202.200.29.1
  6     <1 ms    <1 ms    <1 ms  202.112.53.141
  7     16 ms    16 ms    16 ms  202.205.13.210
  8     17 ms    16 ms    16 ms  210.200.3.143

Trace complete
```

图 12-43　连接情况

【问题 1】

下列选项中__(1)__是 Windows 中代理服务器软件。

（1）A．wingate　　B．outlook　　C．IIS　　D．winzip

【问题 2】

参照图 12-42 和图 12-43，为 server1 网卡 eth1 配置 Internet 协议属性参数。

IP 地址：__(2)__；

子网掩码：__(3)__；

（3）备选答案：

A．255.255.255.0　　B．255.255.254.0　　C．255.255.255.128

为 server1 网卡 eth0 配置 Internet 协议属性参数。

IP 地址：__(4)__；

子网掩码：__(5)__；

默认网关：__(6)__；

【问题 3】

参照图 12-42 和图 12-43，为 host1 配置 Internet 协议属性参数。

IP 地址：__(7)__；

子网掩码：__(8)__；

默认网关：__(9)__；

例题 7 分析

【问题 1】

本题考查代理软件相关知识，WinGate 作为最早的基于 Windows 平台的代理服务器

软件所取得的成功使它成为了网络连接共享的标准。WinGate 是一款 Internet 共享/代理软件，可让局域网络同时共享一个 Internet 账号。从家庭网络到复杂的企业内网络的共享，WinGate 是一款经济、兼容于 Windows 的因特网共享解决方案。包含代理服务器、防火墙、NAT、DHCP 和 DNS 服务，不需要增加硬件、电话线或额外的 ISP 账号。支持各种因特网联机形式。

【问题 2】【问题 3】

从拓扑图中可以观察出，代理服务器 Server1 的外网网卡标识是 eht0，它连接路由器的 e0 端口，而 eth1 则作为内网网卡，下面连接接入层交换机，内网网段为 192.168.0.0/24。题中指出代理服务器的公网 IP 为 61.194.101.35/24。

另外，此题中还要求了解 tracert 命令的功能及执行结果的分析。tracert 命令显示用于将数据包从计算机传递到目标位置的一组 IP 路由器（网关）地址，以及每个跃点所需的时间。如果数据包不能传递到目标，tracert 命令将显示成功转发数据包的最后一个路由器（网关）。当数据报从我们的计算机经过多个网关传送到目的地时，tracert 命令可以用来跟踪数据报使用的路由（路径）。

执行 tracert 命令的执行结果如图 12-44 所示。从前两项中，可以分析出一些有价值的信息，如：第一条记录显示从主机 host1 开始到第一个网关的路由信息，其中 192.168.1.1 为第一个网关地址，即代理服务器的 eth1 接口 IP 地址；第二条记录显示从主机 host1 开始到第二个网关的路由信息，其中 61.194.101.254 为第二个网关地址，即路由器 e0 端口的 IP 地址。读懂了这两条信息，还需要解决的是：代理服务器内网网卡 eth1 接口 IP 地址（192.168.1.1）应与所有主机处于同一网段（192.168.0.0）方能正常通信。由此可以根据子网划分的最大匹配规则，对上两者进行匹配：

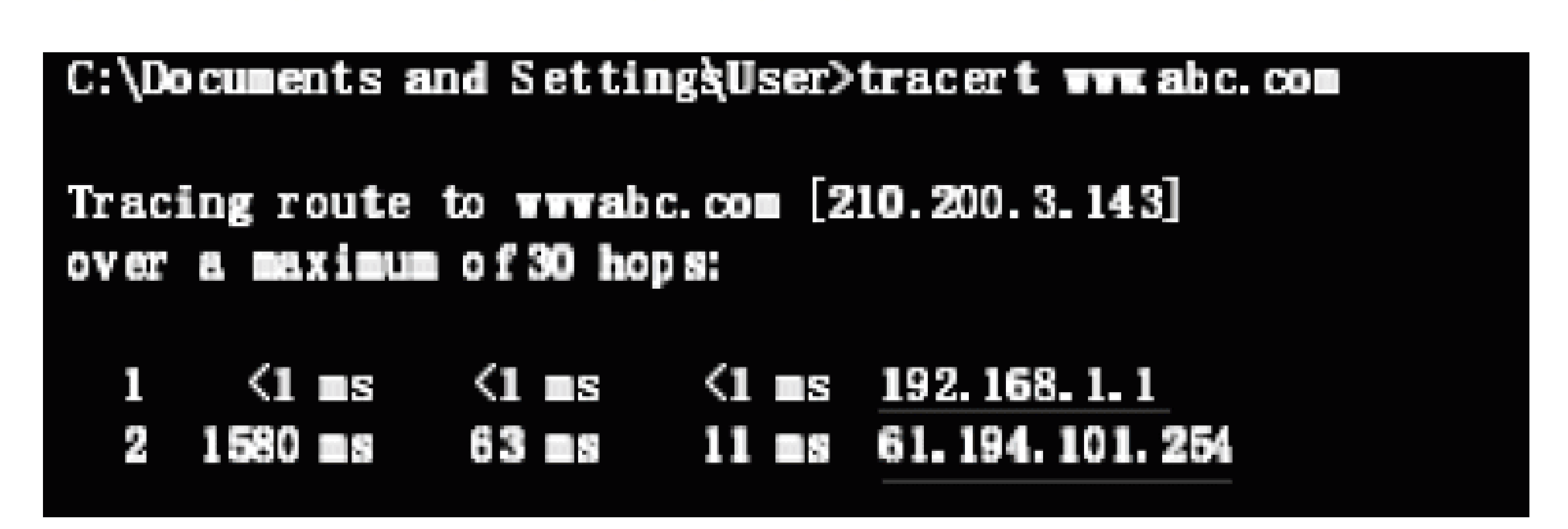


图 12-44 执行结果

192.168.1（000000 1）.1（0000001）

192.168.0（000000 0）.0（0000001）

由此可知，内网网段的子网掩码并不是想当然地默认 C 类掩码 255.255.255.0。应用最大匹配后，可知该网段中前 23 位为网络位，后 9 位为主机位，掩码二进制形式为 11111111.11111111.11111110.00000000，十进制掩码为 255.255.254.0。

根据上面分析，可完成问题 2、问题 3 的配置。

例题 7 答案

【问题 1】

（1）A

【问题 2】

（2）192.168.1.1　（3）B　（4）61.194.101.35

（5）255.255.255.0　（6）61.194.101.254

【问题 3】

（7）192.168.0.18　（8）255.255.254.0　（9）192.168.1.1

例题 8

某公司欲建一小型网站对外发布产品信息，Web 服务器信息描述如下：

（1）操作系统：Windows Server 2003，安装在 D 盘。

（2）双网卡：IP 地址分别是 10.0.0.1 和 212.115.112.31。

（3）网站信息如表 12-7 所示。

表 12-7　网站信息表

名　称	灵便购机网
域名	www.educity.cn
首页	educity.asp
网页存放位置	E:\web

用户可以在浏览器地址栏中输入 http://www.educity.cn:8000 访问该网站。

【问题 1】

填充如图 12-45 所示的网站选项卡。网站“IP 地址”文本框应填入__（1）__，“TCP 端口”文本框应填入__（2）__。

【问题 2】

填充如图 12-46 所示的主目录选项卡。“本地路径”文本框默认情况下为__（3）__，现应填入__（4）__。

（3）A．E:\Internet　B．D:\Internet\website

C．E:\Website　D．D:\Inetpub\wwwroot

【问题 3】

在 E:\web 目录中已有三个文件，如图 12-47 所示。为了使用户能正常访问该网站，在图 12-47 中应如何操作？

【问题 4】

为保障网站的安全性，需要单击图 12-48 中“IP 地址和域名限制”栏内的“编辑”按钮，屏蔽某些恶意 IP 地址。如果要屏蔽 192.168.1.116，在图 12-49 中应如何操作？

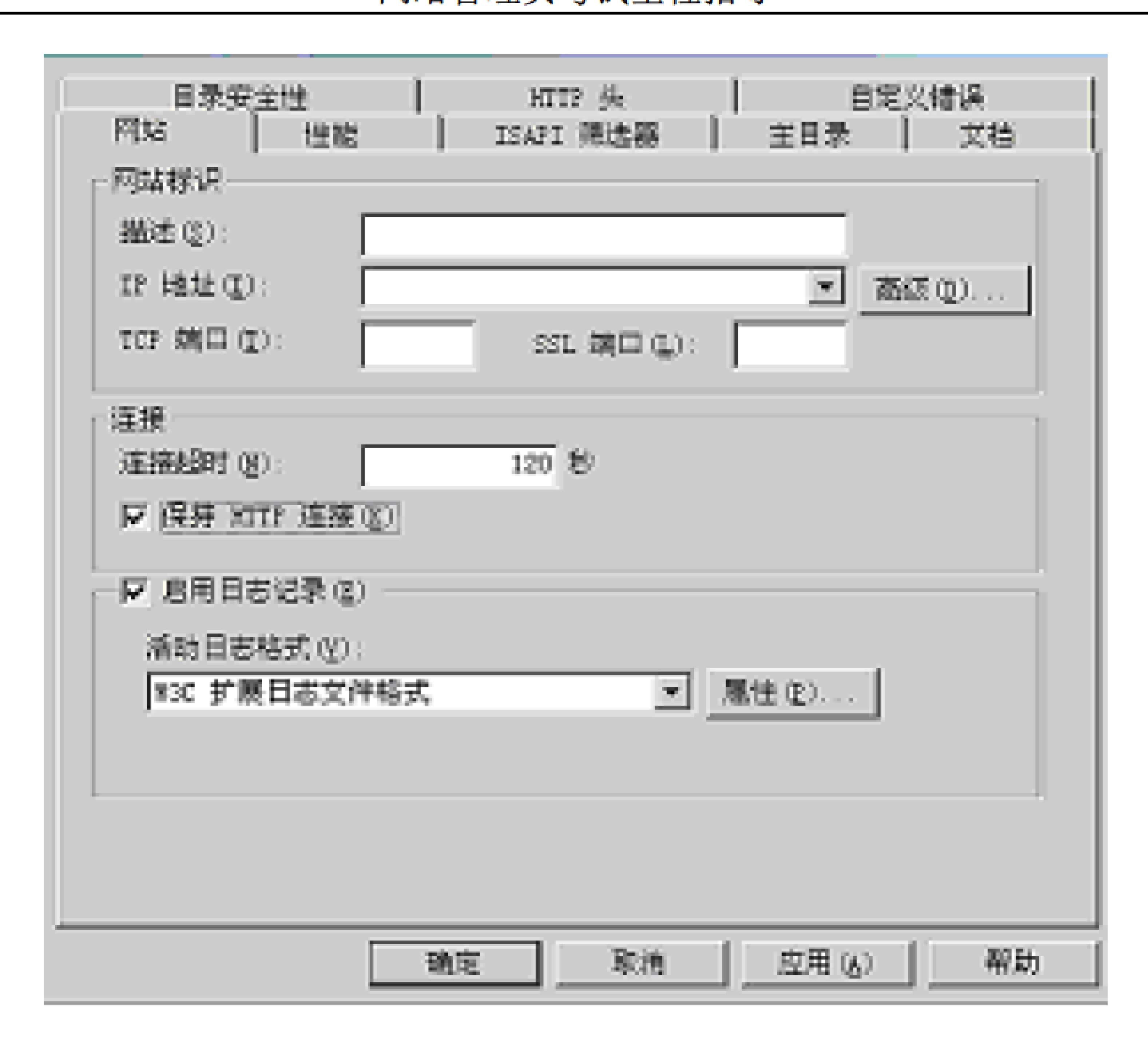


图 12-45 TCP 端口



图 12-46 主目录选项卡

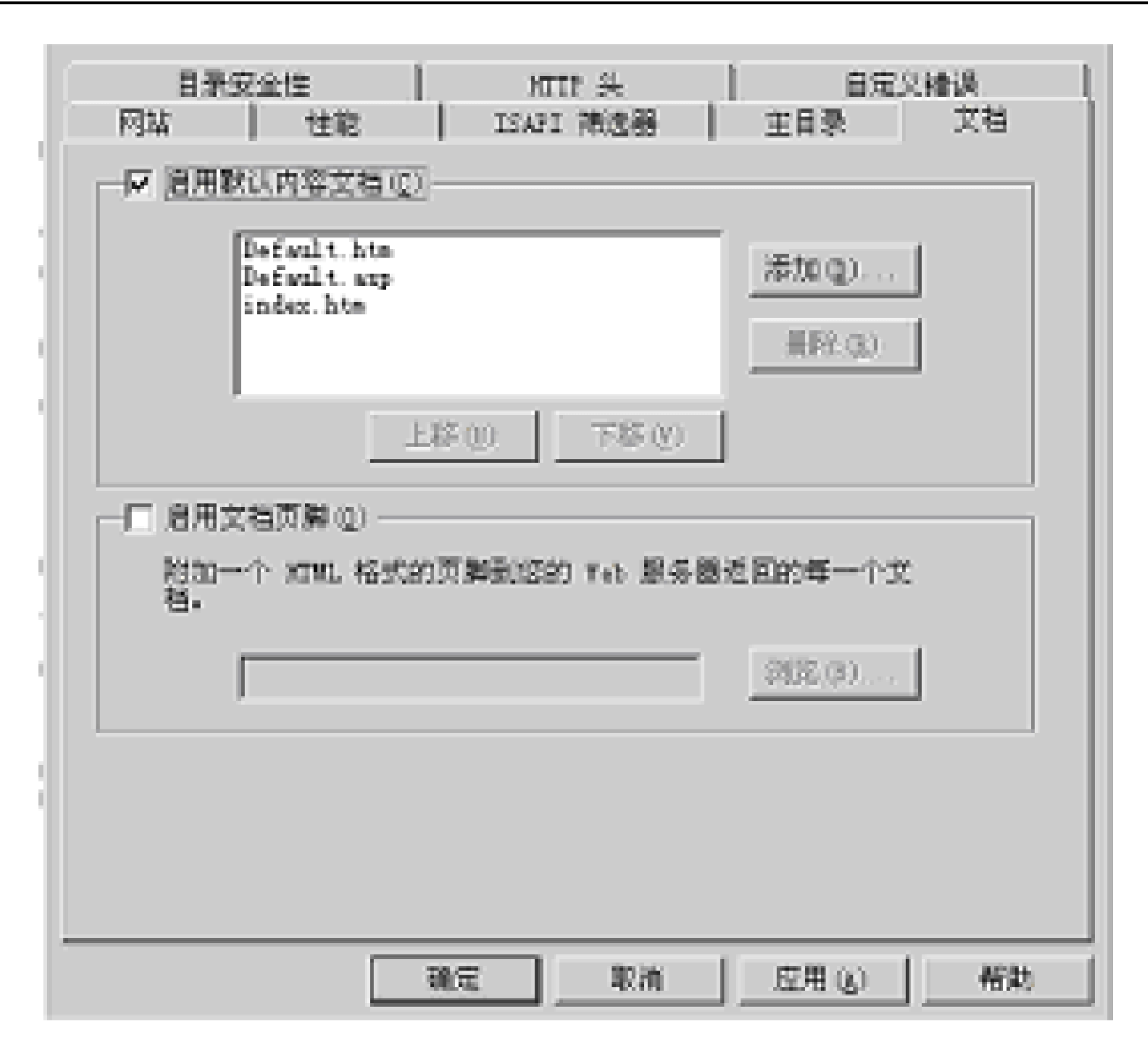


图 12-47　文件的选择

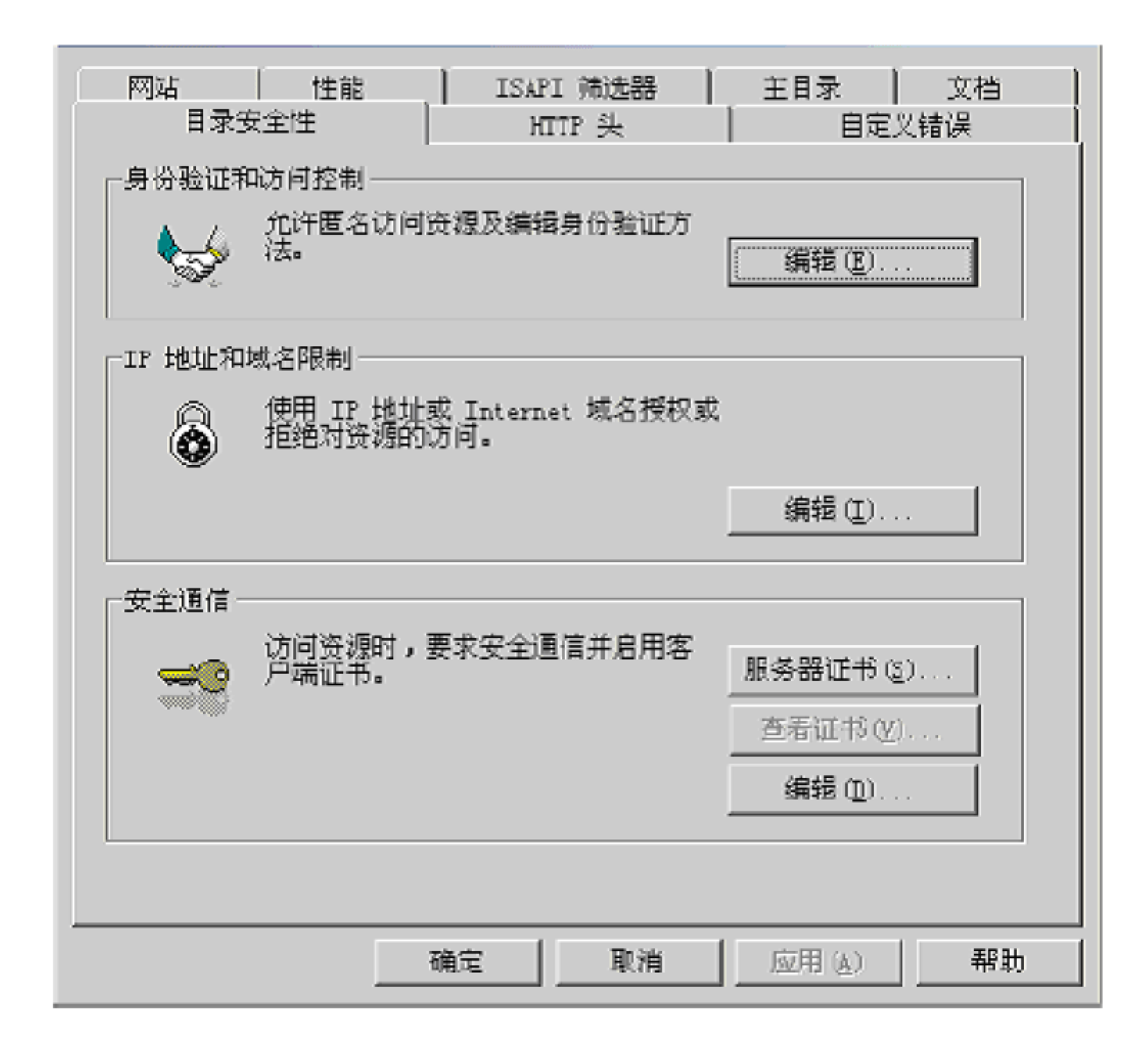


图 12-48　目录安全性

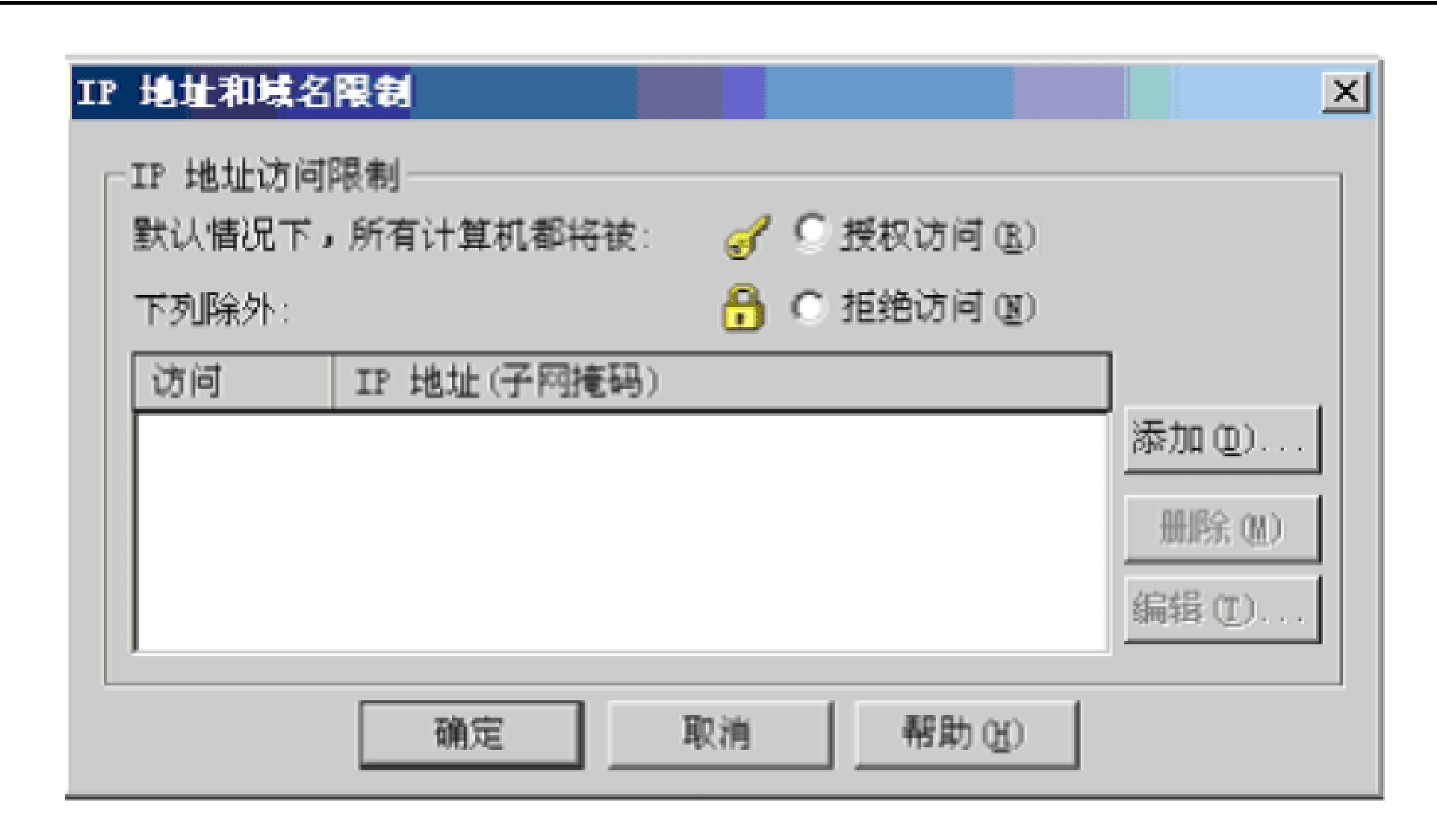


图 12-49 屏蔽操作

例题 8 分析

【问题 1】

本题考查 Windows 图形界面下通过 IIS 配置 Web 服务的相关知识。(1)、(2) 空分别要填入 Web 服务器的 IP 地址及提供服务的端口号。从题中可得知该服务器为对外服务器，对外发布产品信息。因此 IP 地址必须是公网可访问的 IP 地址（212.115.112.31），端口号并非默认 Web 服务的 80 端口，而是通过 8000（http://www.educity.cn:8000）端口进行访问。通过以上分析，不难得出答案。

【问题 2】【问题 3】

这两题分别考查 Web 服务配置过程中 IIS 的默认配置。

Web 服务器默认的目录是系统所在根目录\Inetpub\wwwroot。题中要指定的 Web 目录为 E:\web。

该 Web 站点的首页是 educity.asp，要想访问该 Web 站点时默认跳转到该页面，需要在“文档”选项卡中来进行配置，首先勾选“启用默认文档”复选框，再单击“添加”按钮，将页面文件 educity.asp 添加至列表中。

另外还需要注意：该列表中若有多个页面文件，则是按照从上到下的优先级别连接，因此为了正常快速访问主页，还需要将刚才添加的页面文件列表项移置第一项即可。

【问题 4】

本题考查 Web 目录访问安全性的配置知识。要配置 Web 目录安全性，需要在“目录安全性”选项卡中来进行配置，在设置界面中，可以分别进行身份证与访问控制、IP 地址与域名限制、Web 证书管理等功能。题中要求限制某访问的 IP 地址，只需在如图 2-5 所示的“IP 地址与域名限制”对话中，选择“授权访问”（默认情况下，所有计算机都被授权访问），并添加要屏蔽主机 192.168.1.116 便可完成访问控制。

例题 8 答案

【问题 1】

（1）212.115.112.31　　（2）8000

【问题 2】

（3）D　　（4）E:\web

【问题 3】

单击“添加”按钮，加入 educity.asp 文件，上移至顶端。或依次删除上述三个文件，单击“添加”按钮，加入 educity.asp 文件。

【问题 4】

选中“授权访问”，单击“添加”按钮，加入 IP 地址 192.168.1.116。

【问题 5】

（5）C

第 13 章　网络接入与服务

本章要重点掌握几种常见的接入网技术，特别是电话线、HFC、FTTx+LAN、xDSL接入技术等。根据对考试大纲的分析，并结合历年考试进行验证，本章的出题趋向将偏向基础知识与理论，相对而言其重要性在下降，在复习时应该重点在于对基础概念的记忆。

13.1　各种接入 Internet 的方式

目前接入 Internet 的主要方式有 PSTN、ISDN、ADSL、FTTx＋LAN 和同轴＋光纤接入等 5 种。

1．PSTN 接入

PSTN 是公众电话网（Public Switching Telephone Network）的简称，通过 PSTN 接入是指利用电话线拨号接入 Internet，通常计算机需要安装一个 MOEDEM（调制解调器），将电话线插入到 MOEDEM 上，在计算机上利用拨号程序输入接入号码（如 163，169）进行接入。其速度较低，一般低于 64Kbps。

2．ISDN 接入

ISDN（Integrated Services Digital Network，综合业务数字网）俗称一线通，是在现有的市话网基础上构造的纯数字方式的“综合业务数字网”，能为用户提供包括话音、数据、图像和传真等在内的各类综合业务。ISDN 的基本速率接口（BRI）为 2B＋D 信道，共 144Kbps 带宽，RJ-45 接口；最高可提供 30BD 的带宽，也称做一次群速率接口（PRI），是通过 T-1（E-1）电路传送的标准 ISDN 业务。PRI 通过 30 个分立的或组合的 64Kbps 信道和一个 16Kbps 的 D 信道提供最高达 2.048Mbps 的传输速率。ISDN 的 B 信道是基本信道，提供 64Kbps 带宽来传送语音或数据资料；其 D 信道作为控制信道，提供 16Kbps 或 64Kbps 的带宽，在 ISDN 网络端与用户端之间传输旁带信号，此通道也可用于传输 X.25 资料，但需交换机支持。

3．ADSL 接入

ADSL（Asymmetrical Digital Subscriber Loop，非对称数字用户线路）特点是上行速度和下行速度不一样，并且往往是下行速度大于上行速度。从 1989 年以来，ADSL 走过了一个漫长的历程。下行速率从 1.5Mbps 提高到 9Mbps（当然这是以缩短传输距离为代价的），上行速率也已经提高到 640Kbps。ADSL 的服务端设备和用户端设备之间通过普通的电话铜线连接，无须对入户线缆进行改造就可以为现有的大量电话用户提供 ADSL

宽带接入。随着标准和技术的成熟及成本的不断降低，ADSL 日益受到电信运营商和用户的欢迎，成为接入 Internet 的主要方式之一。

4．FTTx＋LAN 接入

所谓光纤通信，是指利用光导纤维（简称为光纤）传输光波信号的一种通信方法。相对于以电为媒介的通信方式而言，光纤通信的主要优点包括：传输频带宽，通信容量大；传输损耗小；抗电磁干扰能力强；线径细，重量轻；资源丰富等。

1）FTTx 技术

随着光纤通信技术的平民化，以及高速以太网的发展，现在许多宽带智能小区就是采用以千兆以太网技术为主干、充分利用光纤通信技术完成接入的。

实现高速以太网的宽带技术常用的方式是 FTTx＋LAN，即光纤＋局域网。根据光纤深入用户的程度，可以分为五种：

- FTTC（Fiber To The Curb）：光纤到路边。
- FTTZ（Fiber To The Zone）：光纤到小区。
- FTTB（Fiber To The Building）：光纤到楼；
- FTTF（Fiber To The Floor）：光纤到楼层。
- FTTH（Fiber To The Home）：光纤到户。

2）无源光网技术

无源光网（PON）是实现 FFTB 的关键性技术。其在光分支点不需要节点设备，只需安装一个简单的光分支器即可，因此具有节省光缆资源、带宽资源共享、节省机房投资、设备安全性高、建网速度快、综合建网成本低等优点。目前无源光网 PON 技术主要有 APON 和 EPON 两种：

- APON：ATM-PON 基于 ATM 的无源光网络。分别选择 ATM 和 PON 作为网络协议和网络平台，其上、下行方向的信息传输都采用 ATM 传输方案，下行速率为 622Mbps 或 155Mbps，上行速率为 155Mbps。光节点到前端的距离可长达 10～20km，或者更长。采用无源双星型（PDS）拓扑，使用时分复用和时分多址技术。可以实现信元中继、局域网互联、电路仿真、普通电话业务等。
- EPON：Ethernet-PON，基于以太网的无源光网络。是以太网技术发展的新趋势，其下行速率为 1000Mbps 或者 100Mbps，上行为 100Mbps。在 EPON 中，传送的是可变长度的数据包，最长可为 65 535 个字节；而在 APON 中，传送的是 53 个字节的固定长度信元。它简化了网络结构、提高了网络速度。

5．同轴＋光纤接入

同轴光纤技术 HFC 是将光缆敷设到小区，然后通过光电转换节点，利用有线电视 CATV 的总线式同轴电缆连接到用户，提供综合电信业务的技术。这种方式可以充分利用 CATV 原有的网络，由于其建网快、造价低等特点使其逐渐成为最佳的接入方式之一。HFC 是由光纤干线网和同轴分配网通过光节点站结合而成，一般光纤干线网采用星型拓

扑，同轴电缆分配网采用树型结构。

在同轴电缆的技术方案中，用户端需要使用一个称为 Cable Modem（电缆调制解调器）的设备，它不单纯是一个调制解调器，还集成了调谐器、加/解密设备、桥接器、网络接口卡、虚拟专网代理和以太网集线器的功能于一身，它无须拨号、可提供随时在线的永远连接。其上行速度已达 10Mbps 以上，下行速率更高。

其采用的复用技术是 FDM（频分复用技术），使用的编码格式是 64QAM 调制。

13.2 广域网技术

本节将介绍几种比较常见的广域网技术。

13.2.1 异步传输模式

本知识点的内容包括信元及信元交换的基础概念、虚电路技术、信元头、AAL 适配层和 AAL 高层、ATM 的拥塞控制、ATM 的协议单元、子层、复用方式、信元速度和 ATM 适配层、ATM 的虚通道和虚信道知识、ATM 信元交换基础知识。

1．同步传输和异步传输

电路交换网络都是按照时分多路复用的原理将信息从一个节点送到另一个节点的。根据工作模式的不同，可以分为两种：

（1）同步传输模式 STM：根据要求的数据速率，将一个逻辑信道分配为 1 个以上的时槽，在连接存在期时，时槽是固定分配的，即采用的是同步时分复用模式。

（2）异步传输模式 ATM：采用了与前面的不同方法分配时槽，它把用户数据组成为 53Byte 的信元，信元随机到达，中间可以有间隙，信元准备好就可以进入信道，即采用的是统计时分复用模式。

在 ATM 中，信元不仅是传输的基本单位，也是交换的信息单位，它是虚电路式分组交换的一个特例。与分组相比，由于信元是固定长度的，因此可以高速地进入处理和交换。ATM 的典型数据速率为 150Mbps，ATM 是面向连接的，所以在高速交换时要尽量减少信元的丢失。

2．ATM 的分层体系结构

ATM 的层次结构及它们的功能如表 13-1 所示。

表 13-1 ATM 层次结构

层　　次	子　　层	功　　能	与 OSI 对应
高层		对用户数据的控制	高层
ATM 适配层	汇聚子层（CS）	为高层数据提供统一接口	第四层
	拆装子层（SAR）	分割和合并用户数据	

续表

层　次	子　层	功　能	与 OSI 对应
ATM 层		虚通道和虚信道的管理；信元头的组装和拆分；信元的多路复用；流量控制	第三层
物理层	传输会聚子层（TC）	信元校验和速率控制 数据帧的组装和分拆	第二层
	物理介质子层（PMD）	比特定时 物理网络接入	第一层

1）ATM 物理层

物理介质相关子层（PMD）：规定了传输介质、信号电平、比特定时等。例如基于 5 类双绞线或光纤可达到 155.52Mbps、622.08Mbps、2488.32Mbps（SONET 标准）；在 T3 信道上可达 44.736Mbps，在 FDDI 上达到 100Mbps。

传输聚合子层：提供了与 ATM 层的统一接口，该层完成类似数据链路层的功能。

2）ATM 层

ATM 层相当于网络层的功能，它通过虚电路技术提供面向连接的服务。在 ATM 中，虚电路有两级，分别是虚通路（VP）和虚信道（VC）。虚信道与 X.25 的虚电路相当，而虚通道则是由多条虚信道捆绑在一起形成的。53 字节的 ATM 的信元，是由 5 个字节的信元头和 48 个字节的数据组成的。在信元头中，有一些比较重要的字段需要掌握：

- 虚通路标识符（VPI）：8bit 或 12bit，常用是 8bit，因此一个主机上的虚通路数通常是 256 个。
- 虚信道标识符（VCI）：16bit，因此理论上一个虚通路可以包含 65 536 个虚信道，不过部分信道是用于控制的，并不传送用户数据。
- 8 位头校验和：只对信元头进行校验，采用的是 X^8+X^2+X+1 的 8 位 CRC 校验。
- 信元丢失优先级（CLP）：在网络发生拥塞时提供指导，置为 1 的信元可抛弃。
- 流控标志（GFC）：用于主机和网络之间的流控或优先级控制。
- 负载类型（PTI）：区分不同的拥塞信息。

另外，有一个小知识点：在 ATM 逻辑通道中，是使用 VPI+VCI 的组合来标识连接的，在做 VP 交换或交叉连接时，只需要交换 VPI，无须改变 VCI 的值。

3）ATM 适配层

ATM 适配层（AAL）负责处理高层来的信息，发送方把高层来的数字切成 48 字节长的 ATM 负载，接收方把 ATM 信元的有效负载重新组装成为用户数据包。AAL 支持四种业务，有五种 AAL 层协议分别满足这些业务，如表 13-2 所示。

表 13-2 AAL 五种协议

服务类型	A 类	B 类	C 类	D 类
端到端定时	要求		不要求	
比特率	恒定	可变		
连接模式	面向连接			无连接
适配层协议	AAL1	AAL2	AAL3/4 和 AAL5	

- AAL1：检测丢失和误插入信元，提供固定速率。
- AAL2：用于传输面向连接的实时数据流、无错误检测，只检查顺序。
- AAL3/4：原来是两个不同协议，分别提供 C 和 D 类服务，后来合并为一个，用于面向连接和无连接服务。
- AAL5：它是实现 C、D 两类服务的新协议，它能够应用于 ATM 局域网访问。它采用 32 位 CRC 校验。

4）ATM 高层

ATM 的高层主要规定了 4 类 5 种业务类型来满足不同的 ATM 客户需求，AAL5 种业务类型的特点及适合的应用如表 13-3 所示。

在 ATM 中，信元不仅是传输的基本单位，也是交换的信息单位（它是虚电路式分组交换的一个特例，参见“通信基础”的“交换方式”知识点）。与分组相比，由于信元是固定长度的，因此可以高速地进入处理和交换。ATM 的典型数据速率为 150Mbps，也就是每秒可以有约 36 万（150M/8/53）个信元。ATM 是面向连接的，所以在高速交换时要尽量减少信元的丢失。

表 13-3 AAL 业务类型

业 务 类 型	特 点	适 用 应 用
CBR（固定比特率业务）	没有错误检查、流控和其他处理	交互式语音和视频流
RT-VBR（实时性变化比特率业务）	能够对信元的延迟和延迟变化进行控制	交互式压缩视频信号
NRT-VBR（非实时性变化比特率业务）	能够满足按时提交的需求	多媒体电子邮件
ABR（有效比特率业务）		突发式通信
UBR（不定比特率业务）	发生拥塞，信元可丢弃	IP 分组传送

13.2.2 帧中继

本知识点的重点在于掌握帧中继的特点（特别是工作层次、独有的拥塞控制，以及在流量与差错控制方面的特点），理解帧协议与结构。

帧中继协议在二层实现，没有专门定义物理层接口（可以使用 X.21、V.35、G.703、

G.704 等接口协议），在帧中继之上，可以承载 IP 数据报，而且其他协议甚至远程网桥协议都可以在帧中继上透明传输。它所采用的接口协议体系如图 13-1 所示。

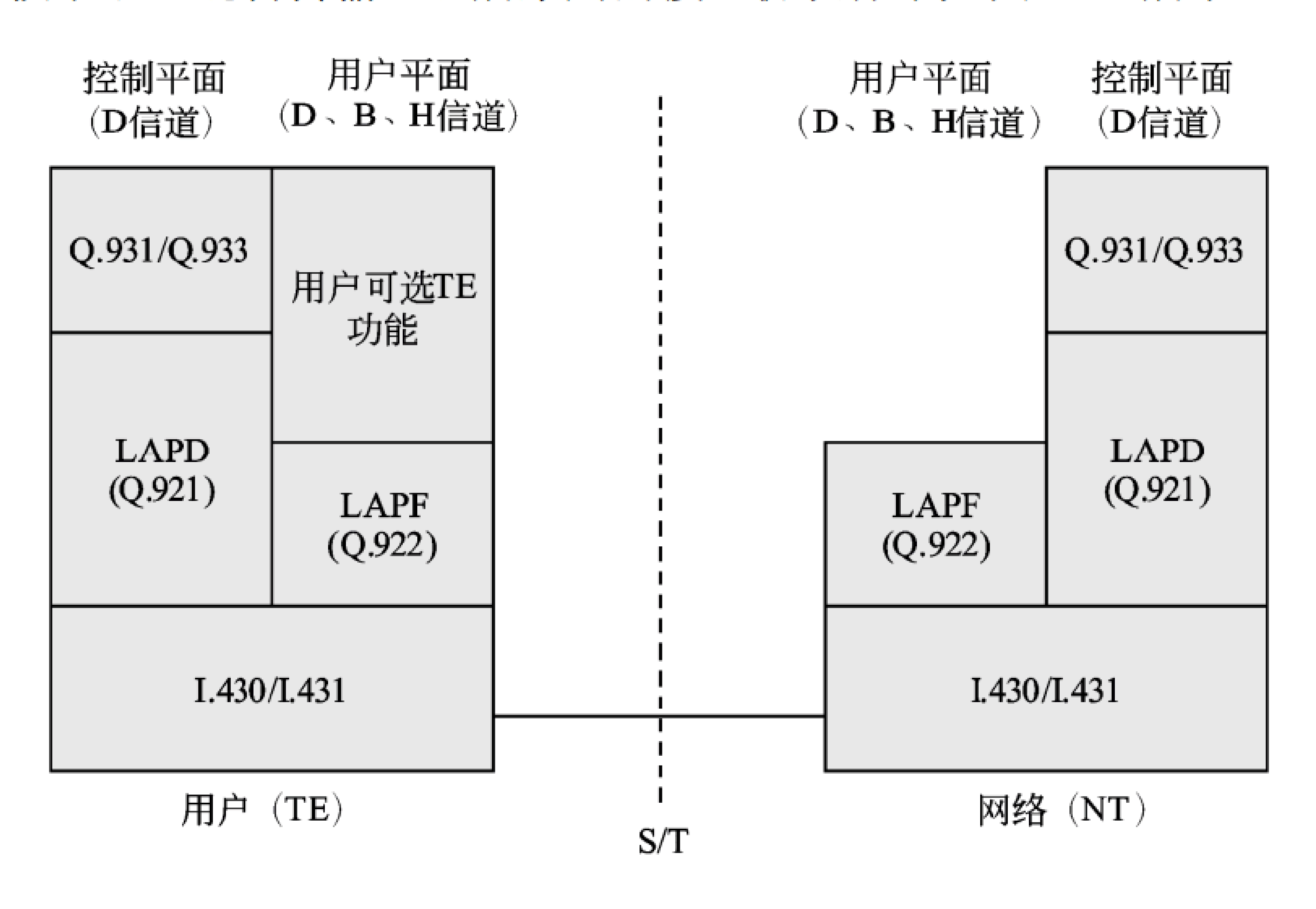


图 13-1　帧中继接口协议体系结构

帧中继使用的最核心协议是公共信道 D 进行信令传输控制协议（Link Access Procedure on the D channel，LAPD），它比 LAPB 更简单，省去了控制字段。在其帧结构中有一些较有特色的地方和一些需要了解的知识点：

（1）信息字段：就是用户要传送的信息，长度是可变的，默认长度为 1600。

（2）帧中继采用了显式拥塞控制机制，在帧头中有 FECN（向前拥塞比特）、BECN（向后拥塞比特）两个特殊字段。如果 FECN 被设置为 1，则说明帧在传送方向上出现了拥塞，该帧到达接收端后，接收方可对数据速率做相应的调整；如果 BECN 被设置为 1，则说明在与传送方向相反的方向上出现了拥塞，该帧到达发送端后，发送端可对数据速率做相应的调整。

（3）帧中继中包括一个 DE（优先丢弃比特），如果设置为 1，当网络拥塞时会优先丢弃。

（4）与 X.25 相类似，帧中继也是使用虚拟电路的方式提供面向连接的服务，在帧头中包括一个 DLCI（数据链路连接标识符）字段，每个 DLCI 都标识出了一个虚电路，其中 DLCI0 是用于信令传输的。

帧中继支持交换虚电路（SVC）和固定虚电路（PVC，永久虚电路）两种虚电路技术：

（1）交换虚电路：控制交换虚电路的信息是在信令信道（DLCI=0）上传送的。这些消息采用的是 LAP-F 协议（LAPF 的帧格式与 LAPD 基本相同，但没有 FECN、BECN 和 DE 字段）。

（2）固定虚电路：帧中继协议在早期并没有建立交换虚电路的信令，只能够通过网络管理建立永久虚电路。PVC 的管理协议控制端到端的连接，是通过带外信令的无编号信息帧传送的。

而基于这两种不同的虚电路技术，帧中继就可以向用户提供不同的服务质量，这些服务质量参数如表 13-4 所示。

表 13-4 服务质量参数

服务质量	缩写	含义
接入速度	AR	指 DTE 可获得的最大速率
约定突发量	Bc	指在测定时间内允许发送的数据量，=CIR×时间
超突发量	Be	指在测定时间内超出 Bc 部分的数据量→尽力传送。Be＝EIR×时间
约定数据速率	CIR	正常状态下的数据速率
扩展的数据速率	EIR	指允许用户增加的数据速率

使用帧中继进行远程连网的主要优点是：透明传输、面向连接，帧长可变，速率高，能够应对突发数据传输，没有流控和重传，开销小。但它并不适用于对延迟敏感的应用（如音频和视频），且无法保证可靠的提交。

13.2.3 同步光网络

对本知识点的理解主要在于同步光纤网络（SONET）和同步数字层级（SDH）的工作原理、优缺点、适用性。

SONET 和 SDH 是一组有关光纤信道上的同步数据传输的标准协议，常用于物理层构架和同步机制。SONET 是由美国国家标准化组织（ANSI）颁布的美国标准版本，SDH 是由国际电信同盟（ITU）颁布的国际标准颁布。两者均为传输网络物理层技术，传输速率可高达 10Gbps，除了使用的复用机制上有所不同，而其余技术均相似。SDH 的网络元素主要有同步光纤线路系统、终端复用器（TM）、分插复用器（ADM）和同步数字交叉连接设备（DXC）。典型的 SDH 应用是在光纤上的双环应用。SDH 每秒传送 8K SDH 帧（STM-N），SDH 是提供字节同步的物理层介质。

IPoverSDH 是以 SDH 网络作为 IP 数据网络的物理传输网络，它使用链路适配及成帧协议对 IP 数据包进行封装，然后按字节同步的方式把封装后的 IP 数据包映射到 SDH 的同步净荷封装（SPE）中。目前广泛使用 PPP 对 IP 数据包进行封装，并采用 HDLC 的帧格式。PPP 提供多协议封装、差错控制和链路初始化控制等功能，而 HDLC 帧格式负责同步传输链路上的 PPP 封装的 IP 数据帧的定界。

SONET/SDH 可以应用于 ATM 或非 ATM 环境。SONET/SDH（POS）上的数据包利用点对点协议（PPP），将 IP 数据包映射到 SONET 帧负载中。在 ATM 环境下，SONET/SDH 线路连接方式可能为多模式、单模式或 UTP。SONET 的传输速率是基本比特率

51.840Mbps 的多倍速率，或是 STS-1。而 SDH 是基于 STM-1，数据传输率为 155.52Mbps，与 STS-3 相当。

目前常用的 SONET/SDH 数据传输率如表 13-5 所示。

表 13-5　SONET/SDH 数据传输率列表

SONET 信号	比特率 Mbps	SDH 信号	SONET 性能	SDH 性能
STS–1 和 OC–1	51.840	STM–0	28 DS–1s 或 1 DS–3	21 E1s
STS–3 和 OC–3	155.520	STM–1	84 DS–1s 或 3 DS–3s	63 E1s 或 1 E4
STS–12 和 OC–12	622.080	STM–4	336 DS–1s 或 12 DS–3s	252 E1s 或 4 E4s
STS–48 和 OC–48	2488.320	STM–16	1344 DS–1s 或 48 DS–3s	1008 E1s 或 16 E4s
STS–192 和 OC–192	9953.280	STM–64	5376 DS–1s 或 192 DS–3s	4032 E1s 或 64 E4s
STS-768 和 OC-768	39 813 120	STM-256	21 504 DS–1s 或 768 DS–3s	16 128 E1s 或 256 E4s

13.3　互联网服务供应商

ISP 的是 Internet Service Provider 缩写，翻译为互联网服务提供商，即向广大用户综合提供互联网接入业务、信息业务和增值业务的电信运营商。ISP 是经国家主管部门批准的正式运营企业，享受国家法律保护。

ICP（Internet Content Provider，互联网内容提供商）是向广大用户综合提供互联网信息业务和增值业务的电信运营商。ICP 同样是经国家主管部门批准的正式运营企业，享受国家法律保护。国内知名 ICP 有新浪、搜狐、163、21CN、希赛等，河南省知名 ICP 有河南通信公司下属的河南信息港、商都信息港，以及 17 个地市信息港等等。

ASP（Application Service Provider，应用服务提供商）是为各种各样的商务客户和事务客户提供其所需的应用，并且这种应用通过托管或者租用的形式实现，而不是使用传统的购买方式或者用户定制开发的形式实现的，从而使客户的应用开发成本大幅度下降。

13.4　例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 5 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

下列有关广域网的叙述中，正确的是__（1）__。

（1）A．广域网必须使用拨号接入

B．广域网必须使用专用的物理通信线路
C．广域网必须进行路由选择
D．广域网都按广播方式进行数据通信

例题 1 分析

广域网有多种接入方式，例如 PSTN、ISDN、DDN、X.25 和 Frame-Relay（帧中继）等，支持的协议有 PPP、HDLC、MPFR、SLIP 和 X.25 等，因此显然不是必须使用拨号接入的。而且广域网大部分是点对点通信，在带宽资源比较珍贵的广播网，显然是不会采用广播方式进行数据通信的。另外，广域网的介质可以有光纤和铜缆，而且还有无线的介质，因此也不是必须使用专用的物理通信线路的。

而广域网是用来连接多个网络的，并在很多情况下还涉及异构的网络，因此大多工作在网络层之上，因此是肯定需要进行路由选择的。

例题 1 答案

（1）C

例题 2

在同步数字系列（SDH）标准中，STM-64 的数据速率为__（2）__。

（2）A．622Mbps　　B．1.5Gbps　　C．10Gbps　　D．100Gbps

例题 2 分析

SDH 称为同步数字层级。它是光数字传输体系的国际标准，其速率从 155.520Mbps 到 2.5 Gbps 以至更高。ITU-T 定义了 SDH 的一系列速率标准如表 13-6 所示。

表 13-6　SDH 系列速率标准

SDH 标准	传 输 速 率
STM-1	155.52Mbps
STM-4	622.08Mbps
STM-16	2.48832Gbps
STM-64	9.95328Gbps

例题 2 答案

（2）C

例题 3

关于 ADSL 接入技术，下面的论述中不正确的是__（3）__。

（3）A．ADSL 采用不对称的传输技术
B．ADSL 采用了时分复用技术
C．ADSL 的下行速率可达 8Mbps
D．ADSL 采用了频分复用技术

例题 3 分析

ADSL 的全称是非对称数字用户环路；它是一种不对称的传输技术，上行速率为 512Kbps～1Mbps，下行速率为 1～8Mbps；它使用 FDM（频分多路复用）和回波抵消技术实现频带分隔，线路编码为 DMT 和 CAP。

例题 3 答案

（3）B

例题 4

下面的选项中，属于分组交换网的是__（4）__。

（4）A．ISDN　　B．帧中继

C．PPP　　D．HDLC

例题 4 分析

分组交换网是继电路交换网和报文交换网之后一种新型交换网络，它主要用于数据通信。分组交换是一种存储转发的交换方式，它将用户的报文划分成一定长度的分组，以分组为存储转发，因此，它比电路交换的利用率高，比报文交换的时延要小，而具有实时通信的能力。分组交换利用统计时分复用原理，将一条数据链路复用成多个逻辑信道，最终构成一条主叫、被叫用户之间的信息传送通路，称之为虚电路（V.C）实现数据的分组传送。

ISDN 是综合业务数字网，就是采用的数字交换和数字传输的电信网的简称，中国电信将其俗称为“一线通”。ISDN 是以电话综合数字网为基础发展而成的通信网，能提供端到端的数字连接，可承载话音和非话音业务，用户能够通过多用途用户——网络接口接入网络。ISDN 采用数字传输和数字交换技术，将电话、传真、数据、图像等多种业务综合在一个统一的数字网络进行传输和处理，向用户提供基本速率（2B＋D，144Kbps）和一次群速率（30B＋D，2Mbps）两种接口。基本速率接口包括两个能独立工作的 B 信道（64Kbps）和一个 D 信道（16Kbps）。其中 B 信道一般用来传输话音、数据和图像，D 信道用来传输信令或分组信息。

帧中继是一种数据包交换技术，与 X.25 类似。它可以使终端站动态共享网络介质和可用带宽。帧中继采用以下两种数据包技术：（1）可变长数据包；（2）统计多元技术。它不能确保数据完整性，所以当出现网络拥塞现象时就会丢弃数据包。但在实际应用中，它仍然具有可靠的数据传输性能。

高级数据链路控制协议（High Level Data Link Control protocol，HDLC）是一种数据链路层协议，促进传送到下一层的数据在传输过程中能够准确地被接收（也就是差错释放中没有任何损失并且序列正确）。HDLC 的另一个重要功能是流量控制，换句话说，一旦接收端收到数据，便能立即进行传输。

点对点协议（Point to Point Protocol，PPP）为在点对点连接上传输多协议数据包提供了一个标准方法。PPP 最初设计是为两个对等节点之间的 IP 流量传输提供一种封装

协议。在 TCP-IP 协议集中它是一种用来同步调制连接的数据链路层协议（OSI 模式中的第二层），替代了原来非标准的第二层协议，即 SLIP。

例题 4 答案

（4）B

例题 5

用户采用 ADSL 虚拟拨号接入因特网，联网时需要输入__（5）__。

（5）A．ISP 的市话号码　　B．ISP 的网关地址

C．用户账号和密码　　D．用户的 IP 地址

例题 5 分析

ADSL 虚拟拨号就是在 ADSL 的数字线上进行拨号，不同于模拟电话线上用调制解调器的拨号，而采用专门的协议 PPP over Ethernet（PPPoE），拨号后直接由验证服务器进行检验，用户需输入用户名与密码，检验通过后就建立起一条高速的用户数字链路，并分配相应的动态 IP。虚拟拨号用户需要通过一个用户账号和密码来验证身份，这个用户账号和 163 账号一样，都是用户申请时自己选择的，并且这个账号是作了限制的，只能用于 ADSL 虚拟拨号，不能用于普通 MODEM 拨号。ADSL 虚拟拨号的宽带接入方式是目前国内宽带运营商提供的主流方式，需要采用宽带路由器的 ADSL 虚拟拨号接入主要是以太网接口没有内置路由功能的 ADSL MODEM。

例题 5 答案

（5）C

第 14 章　网页编程技术

在网络管理员考试中，要求能够掌握 Web 网络的规划、建设、管理与维护的基础知识，并且能够使用 HTML 或相关的工具软件进行基本的网页制作，了解 JSP，ASP，PHP 等动态网页编程技术的基本概念。本章的试题大约占 5 分，占上午考试的 7%左右。而在下午考试中，历年均以一个大题（15 分）的比例出现。本章重点在于了解 HTML 语言的作用，掌握 HTML 的结构标记、常用标记、熟悉样式单，掌握图形、表格、音/视频，表单的开发方法与开发工具，以及 ASP 内置对象的使用，数据库链接的创建，数据查询与表的遍历，数据的页面显示等。另外还对 JSP/PHP 等动态网页技术，XML 标记语言要有一定了解。

14.1　网页制作工具的选择

本知识点在于了解几种主流的网页设计工具及辅助工具的特性及工具的选用。

1．FrontPage

FrontPage 用于设计和制作网页，其中 FrontPage 2007 是办公套装软件 Office 2007 中的成员之一，是目前最流行的网页制作软件之一，其强大的功能深受广大网页制作者喜爱。

2．Dreamweaver

它是 Macromedia 推出的所见即所得网页编辑器，支持最新的 DHTML 和 CSS 标准。它采用了多种先进技术，能够快速高效地创建极具表现力和动感效果的网页，使网页创作过程变得简单无比。不仅提供了强大的网页编辑功能，而且提供了完善的站点管理机制，可以说，它是一个集网页创作和站点管理两大利器于一身的超重量级的创作工具。

3．Flash

Flash 是 Macromedia 公司开发的集动画制作、网页设计和多媒体应用为一体的优秀应用软件，为原本沉寂的网络世界带来了无限的生机和活力，现在最新的版本是 Flash CS4。用 Flash 可制作交互式的动画和电影，这些动画和电影可以插入到网页中，也可以单独成为动态网页，同时，它还自带了功能强大的 ActionScript 编译器，扩展了动画的功能，与网络应用集成得更加紧密。

4．Fireworks

Fireworks 是第一个完全为网页制作者设计的软件。作为一个图像处理软件，Fireworks 能够自由地导入各种图像（如 Macintosh 的 PICT、FreeHand、Illustrator、

CorelDraw8 等矢量文件、Photoshop 文件、GIF、JPEGBMP、TIFF），甚至是 ASCII 的文本文件，而且 Fireworks 可以辨认矢量文件中的绝大部分标记以及 Photoshop 文件的层。而作为一款为网络设计而开发的图像处理软件，Fireworks 能够自动切图、生成鼠标动态感应的 JavaScript 等等，而且 Fireworks 具有十分强大的动画功能和一个几乎完美的网络图像生成器（Export 功能）。

5．文本编辑器（Notepad）

用文本编辑器就可以编写简单的 HTML 文件。打开记事本，新建一个文件，然后将以下代码复制到这个新文件，最后将这个文件存成 first.html。

```
<html>
<head>
<title>Title of page</title>
</head>
<body>
This is my first homepage. <b> This text is bold </b>
</body>
</html>
```

要浏览这个 first.html 文件，双击它。或者打开浏览器，在“文件”菜单选择“打开”命令，然后选择这个文件就可以浏览了。

14.2 HTML 基础知识

本知识点重点在于 HTML 的基础知识，主要包括常用标记、多媒体网页、表格插入、表单和框架，以及 CSS 样式。

14.2.1 常见标记

HTML（超文本标记语言）是生成活动文档的代码系统。HTML 文档实际上是普通文本文件，没有图形、声音、影像、动画，但包含指向这些类型文件的“指针”或链接。HTML 本身是由标识 HTML 文档元素、特性的标记（tag）和属性（attribute）构成的代码系统。HTML 标记能够标识逻辑文档部件，即文档中的主要结构组件，如标题、清单和段落。这些结构组件构成 HTML 文档。

1．结构标记

结构标记向浏览器提供关于文档特性的信息，例如 HTML 版本、文档的标题等。虽然结构标记也是 HTML 文档的一部分，但大部分都是不显示在浏览器中的。HTML 中有五个最基本的结构标记：

1）<!DOCTYPE…>标记

用来向浏览器说明文档遵循的 HTML 版本，在此标记中关键的部分是 DTD（文档

类型定义）元素。例如：

```
<!DOCTYPE HTML PUBLIC "-- //W3C//DTD HTML 3.2 Final //EN">
<!DOCTYPE HTML PUBLIC "-- //W3C//DTD HTML 4.0 Final //EN">
```

2）<HTML>标记

用来表示该文档是 HTML 文档。它应位于<!DOCTYPE…>标记之后，而</HTML>则是 HTML 文档的结尾。

3）<HEAD>标记

包含文档的标题、文档使用的脚本、样式定义和文档名信息。它应位于<HTML>和</HTML>之间。

4）<TITLE>标记

它包含文档的标题，要注意这个标题不是出现在浏览器窗口中。它应该位于<HEAD>和</HEAD>之间，例如：

```
<!DOCTYPE HTML PUBLIC "-- //W3C//DTD HTML 4.0 Final //EN">
<HTML>
   <HEAD>
      <TITLE>This is CSAI page</TITLE>
   </HEAD>
</HTML>
```

5）<BODY>标记

该标记中放置要访问者浏览器中显示信息的所有标记和属性。其他的大多数标记都反映于<BODY>标记之内，它位于</HEAD>和</HTML>之间。

2．常用标记和属性

在 HTML 中放入结构标记后，就可以在<BODY>标记之内放入内容了，常用的标记有标题、清单和水平线标记。

1）标题

标题能够分隔大段文字，概述内容，根据逻辑结构安排信息。HTML 中提供了六级标题，<H1>最大，<H6>最小。不过通常在一个文档中最好限制在 2 或 3 级内。在默认情况下对标题都采用左对齐格式，而大多数浏览器都支持其他两种对齐方式，参见表 14-1。

表 14-1　对齐属性

标 题 属 性	效　果
ALIGN=LEFT	标题左对齐
ALIGN=CENTER	标题居中
ALIGN=RIGTH	标题右对齐

2）文档正文

文档正文标记和属性分为两类：一类是段落级标记及属性，用于整段文本的格式化；另一类是字符级标记及其属性，用于单个字母或单词的格式化。

段落级标记用于指定整段文本的格式，主要包括表 14-2 中所列的四种。除了这四种之外，我们还可以在段中使用
来分行。

表 14-2 段落级格式标记

段落级标记	描 述 属 性
<P></P>	将所括文本作为一个段，适用于普通正式文本
<ADDRESS>	用于地址和联系信息，通常显示为斜体字
<BLOCKQUOTE>	用于表示引用文本，通常两边缩排、行间距比普通段落较小
<PRE>	用于排版程序代码之类的信息，通常用定宽字体，字间和行间有足够的间隔

而字符级格式化则用来对字母或单词进行强调，常见的字符级格式化标记如表 14-3 所示。

表 14-3 字符级格式标记

字 符 标 记	效 果	字 符 标 记	效 果
<B>	加粗	<STRONG>	强烈强调
<BLINK>	使文字闪烁	<SUB>	显示为下角标
<CITE>	表示引用	<SUP>	显示为上角标
<CODE>	显示程序代码	<TT>	采用定宽字体
<EM>	强调，常显示为斜体	<U>	采用下划线
<I>	斜体	<VAR>	显示变量或变元

3）清单

清单特别适合提供结构化、易于阅读的信息格式。清单可以分为编号清单（有顺序）和强调符清单（无顺序）两种。

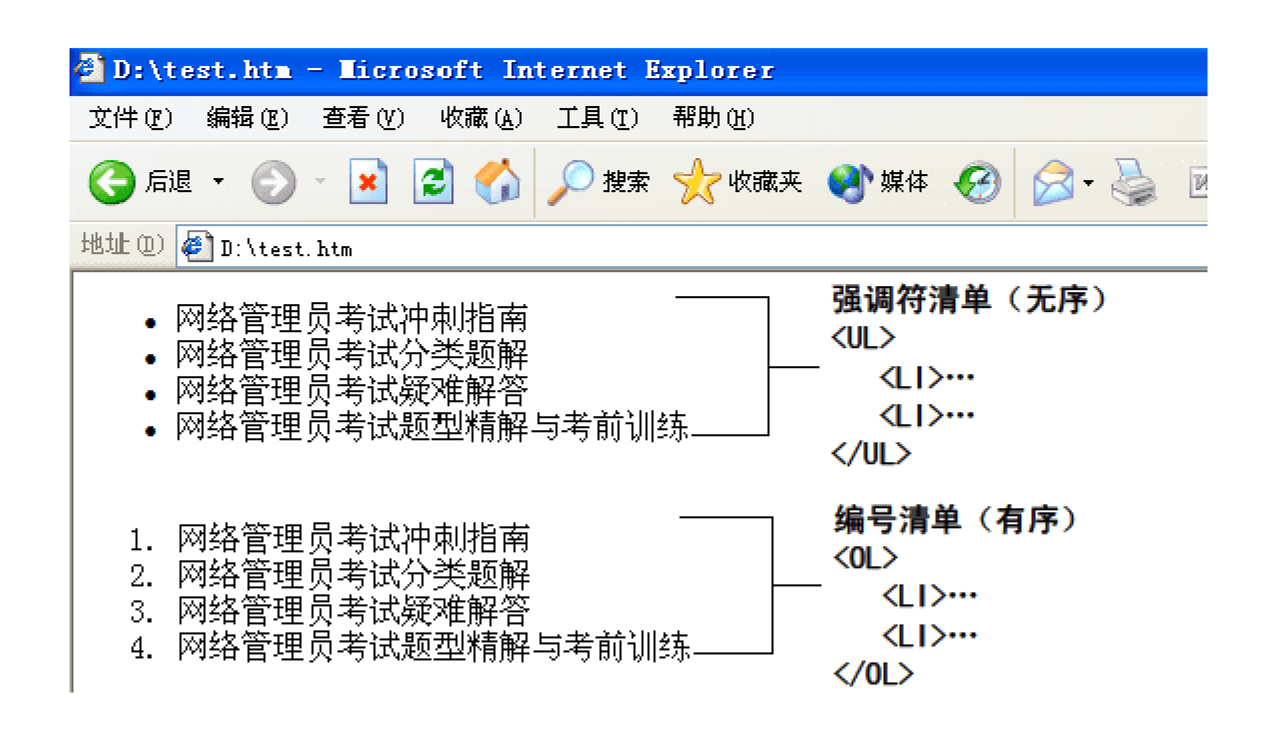


图 14-1 清单标记使用示意

从图 14-1 可以得知，强调符清单和编号清单的项目都是用<LI>定义的，只是清单的定义有些区别，前者为<UL></UL>，后者为<OL></OL>。

可以对清单的外观（使用 TYPE 属性）进行设置：对于编号清单，可以将清单开头的数字或字母设置为 A，a，I，i 或 1（默认值），只需将这些值赋给 TYPE 属性即可；而对于强调符清单则可以使用 DISC、SQUARE、CIRCLE 来表示实心圆心（默认）、实心方形和空心环型三种强调符。另外，对于编号清单，我们还可以使用 START 属性值来指定编号的开始值。TYPE 和 START 属性是 UL 及 OL 标记的属性。而对于<LI>标记，也可以使用 VALUE 属性来设置某个项目的编号。我们还可以通过有序清单的嵌套和不同的 TYPE 属性来生成大纲。

除了<UL>和<OL>之外，还有一种特殊的定义清单，用于提供两级清单。它可以被看成是字典中的项目格式，有词条和定义两个部分。一般用<DL></DL>来定义清单，用<DT>来定义项目，用<DD>来定义内容。

4）水平线

水平线就是分开大段文本的水平线，表示信息主题的转换或帮助改进文档的总体结构。在 HTML 中使用<HR>标记来显示水平线。它常用的属性包括：SIZE=n（定义高度的像素数）、WIDTH=n（定义宽度的像素数）、WIDTH＝“n%”（定义宽度占文档宽度的百分比）、NOSHADE（指定其无阴影），此外还可以使用 ALIGN 属性。

5）修饰性元素

为了使得 HTML 更有表现力，还提供了颜色、字体的设置手段。颜色是最简单的一种美化的手段。<BODY>标记中与此相关的属性包括如表 14-4 所示的属性。

表 14-4　颜色相关属性

属　　性	说　　明
BGCOLOR="#…"	将背景设置为#号后面指定的颜色
TEXT="…"	用颜色名或#RRGGBB 值设置文档中所有文本的颜色
ALINK="…"	用颜色名或#RRGGBB 值设置文档中活动链接的颜色
VLINK="…"	用颜色名或#RRGGBB 值设置文档中访问者最近访问过的链接的颜色
LINK="…"	用颜色名或#RRGGBB 值设置文档中未访问的链接颜色

另外，我们还可以用<FONT>标记来指定文档的字体特性，包括颜色、大小和字体。它包括表 14-5 中的属性。

6）超链接

超链接是 Web 页面中重要的属性，因此在 HTML 中当然有相应的标记，而且提供了同一文档中、同一个文件夹的不同文档中、同一服务器的不同文档中、不同服务器中四种不同情况的链接方式，还可以插入 E-mail 链接，如表 14-6 所示。

表 14-5 颜色相关属性

属 性	说 明
SIZE="…"	指定相对字体大小 1～7，默认值为 3，也可以用+和–指定相对大小
COLOR="…"	用颜色名或#RRGGBB 值指定<FONT>包括的文本颜色
FACE="…"	指定一系列字体类型，按优先级列出

表 14-6 链接到不同位置的文档

位 置	链 接 示 例
同一文档中	<A HREF="#test">
同一文件夹不同文档	<A HREF="test.html#test">
同一服务器的不同文档	<A HREF="test/test.html#test">
不同服务器	<A HREF="www.csai.cn/test/test.html#test">
插入 E-mail 链接	<A HREF=mailto:tangle@csai.cn>

要注意的是，在表 14-6 中，对于同一文档中的链接，是用“#test”给指出锚点。而这个锚点是需要在本文档中定义的，我们称之为命名位置点。例如：

```
<A Name="test">test</A>
```

14.2.2 多媒体网页

在静态网页中，可以嵌入图形、图像、音/视频或动画等媒体，使网页更加形象美观。

1．加入图形

要想使得 Web 页面更加生动，就必须往其中加入图形，插入图形所需使用到的主要标记和属性，具体属性与说明如表 14-7 所示。

表 14-7 图形标记及其属性

标记/属性	说 明
<IMG>	在 HTML 文档中标识图形
ALT="…"	在不能显示图形时显示的替换文本
SRC="…"	指向图形文件的 URL
HEIGHT=n	指定图形高度的像素值
WIDTH=n	指定图形宽度的像素值
BORDER=n	指定图形边框宽度的像素值
ALGIN="…"	指定图形对齐方式：TOP，MIDDLE，BOTTOM，LEFT，RIGHT

除了插入图形这个基本的功能之外，还可以实现以下一些增加的功能。

1）生成图形链接

用图形作为链接对作者和访问提供特有的优势，一张图能顶千句话，放上图形代替大量文字说明很多问题，给其他页面元素留出大量的空间。而要用图形作为链接，实际上很简单，只需将<IMG>标记放在<A>与</A>之间即可，如：

```
<A HREF="test.html"><IMG SRC="test.gif" WIDTH="300" HEIGHT="82"
BORDER="0" ALT="Test"></A>
```

2）生成略图

还可以默认在页面显示出小图，然后将这个小图链接到大图中去，这样就可以减少访问者的下载时间。

3）使用背景图形

大多数浏览器都支持背景图形，即在 HTML 文档的文本后面放上图形或图案。一般来说，背景图形平铺在空间中，用同一个图形的多个备份一个接一个地填满屏幕。要想加入背景图形，只需要<BODY>标记中使用表 14-8 中的背景属性。例如<BODY BACKGROUND="bj1.jpg">。

表 14-8　背景属性

标记/属性	说　　明
BACKGROUND="…"	在 URL 标识 HTML 文档的背景图形
BGPROPERTIES=FIXED	在 IE 中设置背景图形为不平铺、不滚动

4）支持的图形格式

在 Web 上较常见，也是大部分浏览器能够接受的图形格式包括 GIF、JPG 以及 PNG。GIF 是专门用于联机使用的格式，它能够支持动画、透明、图形渐进、无损压缩等。而 JPG 的优点在于颜色的高保真度。而 PNG 组合了 GIF 的大部分优点，而且能够支持高保真的颜色。

2．加入多媒体

随着带宽的日益增加，现在往 HTML 文档中添加多媒体文件已经十分常见了。而常加入的多媒体形式包括动态 GIF、声音、影像、Java 小程序等。而动态 GIF 本身也是图片，因此其添加方法与前面所述添加图形的方法一样。

1）支持的声音格式

在 Web 页面播放声音，能够支持的格式包括 MIDI、AIFF、AU 和 WAV 四种格式。

2）支持的影像格式

能在 Web 页面嵌入的影像文件，主要包括 AVI、MPEG、QuickTime 三种格式。

3）标记与属性

确定了声音/影像文件之后，就可以使用表 14-9 所示的标记和属性，将声音加入到

HTML 文档中去。

表 14-9　多媒体标记和属性

标记/属性	说　　明
<EMBED>	将嵌入对象放在文档中
ALIGN="…"	表示嵌入对象相对于文档边框和周围内容如何放置
HEIGHT="n"	指定嵌入对象的垂直尺寸
HIDDEN	表示嵌入的对象不显示
NAME="…"	给对象一个名称，以便引用
OPTIONAL PARAM="…"	指定可选参数
SRC="URL"	表示要嵌入对象所在文件的相对或绝对位置
WIDTH="n"	指定嵌入对象的宽度
AUTOSTART="…"	指定访问 Web 页面时或单击按钮时是否打开声音文件，TRUE 表示自动启动
HIDDEN="…"	指定声音控制面板是否显示
<BGSOUND>	在文档中嵌入背景声音文件，放在<HEAD>中供 IE 访问者使用
LOOP="{n,INFINITE}"	指定背景声音文件重复次数，默认的 INFINITE 为无穷循环

14.2.3　表格插入

HTML 表格是由行和列构成的。这些行和列构成一个个单元，其中可以放文本或图形。表格可以用来显示复杂的数据，也可以用表格将复杂设计元素放进 Web 页面。

1）生成基本表格

生成最基本的表格的步骤为：首先输入<TABLE>标记，再指定行、列和列标题；然后在表格单元中输入数据。在 HTML 中提供了四个基本表格标记，具体参见表 14-10。

表 14-10　基本表格标记

标　　志	说　　明
<TABLE>	在 HTML 文档中标识表格
<TR>	标识表格中的一行，结束标记</TR>可选
<TD>	标识一行中的单元，结束标记</TD>可选
<TH>	标识一行标题单元，结束标记</TH>可选

假设，我们要生成如表 14-11 所示的表格。

表 14-11　示例表格

学　　号	姓　　名	成　　绩
1	张三	93
2	李四	96

则相应的 HTML 代码则应该为：

```
<TABLE>
<TR>
    <TH>学号</TH>
    <TH>姓名</TH>
    <TH>成绩</TH>
</TR>
<TR>
    <TD>1</TD>
    <TD>张三</TD>
    <TD>93</TD>
</TR>
<TR>
    <TD>2</TD>
    <TD>李四</TD>
    <TD>96</TD>
</TR>
</TABLE>
```

在生成表格之后，可以根据信息改变情况随时增删内容。如果要新增加行，则比较简单，只需再加入一组<TR>、<TD>即可。要增加列则相对更复杂一些，需要在每一行中增加单元，即在每组<TR>中加入一个<TD>。

而删除行与列比增加行与列更容易一些，删除行时一定要删除每个项目的<TD>标记和包围它的<TR>标记，删除列时，则一定要删除<TH>标记和每行的<TD>标记。

2）生成跨行跨列的表格

跨行和跨列就是一个单元占几行或几列单元的位置。如表 14-12 就是一个存在跨行跨列表格的情况。

表 14-12　示例表格

<table>
<tr><th>学　号</th><th>姓　名</th><th>学　科</th><th>子　科　目</th><th>成　绩</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">张三</td><td colspan="2">大学语文</td><td>83</td></tr>
<tr><td>计算机</td><td>数据结构</td><td>90</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">李四</td><td colspan="2">大学语文</td><td>86</td></tr>
<tr><td>计算机</td><td>数据结构</td><td>91</td></tr>
</table>

“学号”、“姓名”两列中，均有跨行的情况，而“学科”和“子科目”两列中，则有跨列的情况。为了指定跨行和跨列，则可以用表 14-13 所示的属性。

表 14-13　基本表格标记

标　　记	说　　明
ROWSPAN=n	用于<TH>或<TD>标记中，表示单元所跨的行数
COLSPAN=n	用于<TH>或<TD>标记中，表示单元所跨的列数

则相应的 HTML 代码则应该为：

```
<TABLE>
<TR>
    <TH>学号</TH>
    <TH>姓名</TH>
    <TH>学科</TH>
    <TH>子科目</TH>
    <TH>成绩</TH>
</TR>
<TR>
    <TD ROWSPAN=2>1</TD>
    <TD ROWSPAN=2>张三</TD>
    <TD COLSPAN=2>大学语文</TD>
    <TD>83</TD>
</TR>
<TR>
    <TD>计算机</TD>
    <TD>数据结构</TD>
    <TD>90</TD>
</TR>
<TR>
    <TD ROWSPAN=2>2</TD>
    <TD ROWSPAN=2>李四</TD>
    <TD COLSPAN=2>大学语文</TD>
    <TD>86</TD>
</TR>
<TR>
    <TD>计算机</TD>
    <TD>数据结构</TD>
    <TD>91</TD>
</TR>
</TABLE>
```

在<TABLE>和</TABLE>中加入<CAPTION>标记，就可以将标题加入到表格中去。

3）生成表格边框

表格边框是表格项目周围的直线，用于分开行、列和单元。默认情况下，显示无边框表格的。在 HTML 中提供了表 14-14 所列出的边框属性（属于<TABLE>标记）。

表 14-14　表格边框属性

属　　性	用　　法
BORDER=n	指定表格边框宽度的像素值，数字越大则越宽，0 表示无边框
BORDERCOLOR="#rrggbb"	指定表格边框颜色名或#rrggbb 数
BORDERCOLORLIGHT="#rrggbb"	指定产生表格三维效果的淡边框颜色
BORDERCOLORDARK="#rrggbb"	指定产生表格三维效果的深边框颜色

4）加入表格背景

除了指定边框颜色外，还可以指定表格背景显示特定颜色或图形，具体属性见表 14-15。

表 14-15　表格背景属性

属　　性	说　　明
BGCOLOR="#rrggbb"	将表格的背景颜色设置为#rrggbb
BACKGROUND="URL"	指定表格的背景图形

5）指定单元格对齐方式

单元对齐指单元内容的水平或垂直对齐，默认情况下是表并没有在单元中水平居中，垂直居中；表格内容在单元中水平左对齐，垂直居中。单元格对齐属性如表 14-16 所示。

表 14-16　单元对齐属性

属　　性	说　　明
ALIGN=n	指定水平对齐方式，LEFT、CENTER 和 RIGHT（左、中、右）
VALIGN=n	指定垂直对齐方式，TOP、MIDDLE 或 BASELINE（顶、中、底）

6）指定单元大小

指定表格单元大小的方法有两种：作为浏览器窗口的百分比，以及指定具体大小（像素值）。可以通过<TH>或<TD>标记的 WIDTH 属性进行设置。单元格大小设置如表 14-17 描述。

表 14-17　单元格大小属性

属　　性	说　　明
WIDTH="n"	指定单元宽度的像素值或占表格宽度的百分比
NOWARP	禁止单元中的文本换行，要求所有文本出现在一行中

7）增加单元间隔和单元填充

单元间隔是单元之间的间隔，单元填充是单元内容与单元边框的间隔，这两个值可以用来设置表格中显示的空白大小。我们可以通过<TABLE>标记的属性来设置，如表14-18 所示。

表 14-18 单元间隔与填充属性

属　　性	说　　明
CELLSPACING=n	指定单元之间的间隔量，像素值
CELLPADDING=n	指定单元内容与单元边框之间的间隔量，像素值

14.2.4 HTML 表单

为了使得 Web 页面与 Web 站点之间实现双向通信，W3C 提出了“表单”技术，我们可以使用 HTML 开发工具来实现表单。

1．表单生成

表单包括可视的（访问者填写）和不可视的（指定服务器如何处理信息）两部分。在表单中通常包括表 14-19 所示的用于收集数据的控件。

生成表单的第一步是插入<FORM></FORM>标记，并加入提交和复位按钮。

表 14-19 表单控件

控　　件	说　　明
提交和复位按钮	用于将表单的信息发送给服务器处理或返回表单初始设置
文本字段	是输入少量文本的区域，用于姓名、搜索项等
选择清单	是让访问者选择一个或几个项目的清单
复选框	让访问者选择清单中的零个、一个或几个项目，用于多项选择
单选钮	让访问者有机会选择单个项目
文本区	是输入大段文本的区域

最基本的表单标记如表 14-20 所示。

表 14-20 基本表单标记与属性

属性/标记	说　　明
<FORM>	在 HTML 文档中生成表单
<INPUT TYPE="SUBMIT" VALUE="…">	提供表单的提交按钮，Value 属性产生 SUBMIT 按钮上的文本
<INPUT TYPE="IMAGE" NAME="POINT" SRC="…" BORDER=0>	提供图形提交按钮，SRC 属性表示图形源文件，BORDER=0 则关掉图形边框

2．输入字段

利用<INPUT>字段的各个属性可以生成其他类型的输入字段，表 14-21 列出了最常用的输入字段标记和属性。

表 14-21　输入字段标记与属性

属性/标记	说　明
<INPUT>	在表单中设置访问者输入的区域
TYPE="…"	设置输入字段的类型，可以取值 TEXT（文本）、PASSWORD（密码）、CHECKBOX（复选框）、RADIO（单选项）、FILE（文件）、HIDDEN（隐藏字段）、IMAGE（图像）、SUBMIT（提交按钮）、RESET（复位按钮）
NAME="…"	处理表单结果
VALUE="…"	提供与 NAME 相关联的内容，该属性用于复选框和单选钮，因为它们不接受其他输入，可将此属性用于文本字段，提供初始输入
SIZE="n"	设置字段的显示长度，这个属性用于文本输入字段
MAXLENGTH="n"	设置可提交的最长的字符集，这个属性用于文本字段
ACCEPT="…"	设置可接受的上传文件的 MIME 类型，可用通配符

下面，我们就以文本字段为例来说明。文本字段是表单中的空白区，用来供访问者输入信息，图 14-2 就是一个使用文本字段的实例。

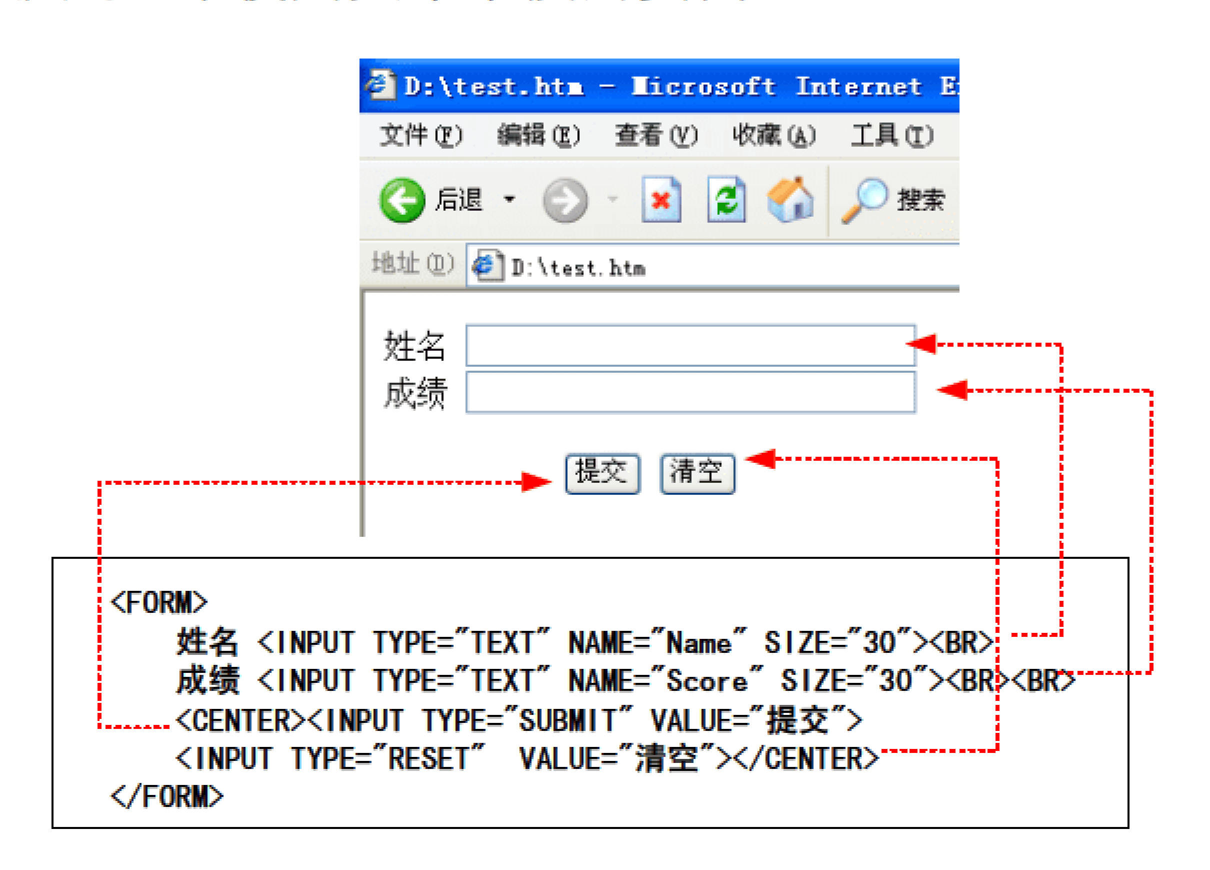


图 14-2　文本字段使用示例

下面则列出了其他一些输入字段的使用示例：

```
========================单选钮========================
<INPUT TYPE="RADIO" NAME="TEST" VALUE="AGREE">赞成<BR>
<INPUT TYPE="RADIO" NAME="TEST" VALUE="OPPOSE">反对<BR>
========================复选框========================
<INPUT TYPE="CHECKBOX" VALUE="Sport">体育<BR>
```

```
<INPUT TYPE="CHECKBOX" VALUE="Shopping">购物<BR>
<INPUT TYPE="CHECKBOX" VALUE="Reading">阅读<BR>
=======================文件字段=======================
<INPUT TYPE="FILE" NAME="Filenew" SIZE="20" ACCEPT="image/*"
```

而另外要说明的是用 HIDDEN 类型说明的隐藏字段是指访问者看不到，但接收表单输入的程序能够识别的信息。通常用来作为提供链接的信息。

3．文本区

如果要在表单中输入大量的文本，那么就可以使用文本区<TEXTAREA>，与其相关的标记和属性如表 14-22 所示。

表 14-22 文本区所用的标记和属性

属性/标记	说　明
<TEXTAREA>	在表单中设置大段文本输入区，文本区的初始内容放在开始和结束标记之间
NAME="…"	建立输入字段的标题，NAME 属性用于表单处理
ROWS="n"	设置显示字段的行数
COLS="n"	设置显示字段的列数

4．字段选择

选择字段是表单开发中最常用最灵活的形式，因为可以让访问者选择一个或几个响应。在 HTML 中列出了选择字段的标记和属性，见表 14-23。

表 14-23 选择字段的标记和属性

属性/标记	说　明
<SELECT>	在表单中设置选择字段区，样子像个下拉清单或大选择字段
NAME="…"	建立输入字段下标题，NAME 属性用于表单处理
SIZE="n"	设置选择字段下拉清单的显示尺寸，默认为 1，如果要显示多个选项，可以修改值
MULTIPLE	将选择字段设置为接受多个选项，这个属性和 SIZE 属性一起设置最大选项数
<OPTION>	标识选择字段中包括的项目，每个项目都要用一个<OPTION>标记
VALUE="…"	提供与 NAME 属性相关联的内容
SELELTED	可以指定默认选项，在表单装入或复位时显示

5．表单处理

一般来说，访问者单击表单上的提交按钮之后，信息发送到 Web 服务器上，由表单 ACTION=属性所指示的程序处理。可以在这个程序中对数据进行各种处理，包括通过 E-mail 将信息发回访问者；将信息输入数据库；将信息发表到新闻组或 Web 页面上；根据输入内容搜索数据库等。

不管如何处理信息，都可以在开始<FORM>标记中加上具体的属性，如表 14-24 所示。

表 14-24　<FROM>标记的属性

属　性	说　明
ACTION="…"	指示 HTTP 服务器上处理表单输出的程序
METHOD="…"	告诉浏览器如何将数据送给服务器（用 POST 方法还是 GET 方法）

14.2.5　CSS 样式

样式单（Cascading Style Sheet，CSS）是一种方便而一致地格式化 HTML 文档的最佳方式。使用样式单可以将形式与内容分离，提高灵活性，减少开发和维护 HTML 文档的时间。连接样式单的方法有四种：一是将样式单嵌入到 HTML 文档中的<HEAD></HEAD>间；二是将样式表存入单独的文件，并将其 import 到 HTML 中，指定样式用于部分 HTML 文档，使用线上样式定义。

1）将样式单嵌入 HTML 文档中

这种方式最简单，只要将<STYLE>标记和样式信息插入到<HEAD></HEAD>间即可，它使用到的标记和属性如表 14-25 所示。

表 14-25　样式单标记及属性

标记/属性	说　明
<STYLE>	指定 HTML 文档的样式单区域
<!--…-->	说明标记，使样式单内容在不支持样式单的浏览器中隐藏起来
TYPE="text/css"	指定样式单类型，text/css 表示层叠样式单；tet/jss 表示 JavaScript 样式单

2）独立存放的样式单

独立存放的样式单就是普通文本文件，只包括样式定义。当开发完独立的样式单后，就可以使用引入或链接的方法关联到 HTML 中。

引入法适用于需要开发多个样式单页面而各有不同的功能的情况。只需在 HTML 文档中使用“@import url（…）”即可，例如：

```
<STYLE>
<!--
@import url('red.css');
-->
</STYLE>
```

而链接法则可以使访问者能够选择特定页面所用的样式单，它采用的是<LINK>标记，具体而言如表 14-26 所示。

表 14-26 链接样式单的标记及属性

标记/属性	说 明
<LINK>	链接样式单
REL="StyleSheet"	指定引用的文件为样式单
TYPE="text/css"	指定样式单类型
HREF="URL"	指定样式单源文件的 URL
TITLE=""	命名样式单

3）对部分文档应用样式单

也可以在 HTML 文档的特定部分包含样式单，这种情况称为样式类（Style class），样式类在样式单中使用。常用于样式类的标记和属性如表 14-27 所示。

表 14-27 链接样式单的标记及属性

标记/属性	说 明
<SPAN>	保存样式属性，应用在单词和字母周围
<DIV>	保存样式属性，应用于段落或其他周围
CLASS="…"	引用样式类，将其用于 HTML 文档的指定部分
ID="uniquen"	指定与特定样式定义相关联的唯一名称，只能在样式单中使用一次

14.3 动态编程技术

本节主要内容包括动态网页基础、ASP/JSP 动态编程基本语法与网页编程实践技术。

14.3.1 动态编程基础

本知识点重点在于掌握 JSP，ASP 和 XML 等动态网页技术的基本概念。随着 Web 应用程序的飞速发展，静态的 HTML 对于显示相对静态的内容是不错的选择，但对于交互式的 Web 应用程序的创建却显得十分不足。这也就催生了动态网页技术，主要包括 PHP，ASP，JSP，以及新的 ASP.NET，XML 技术等。

动态 Web 技术是指内容信息不是被存储在磁盘上，而是根据需要再进行生成。而根据生成发生的位置不同，可以分为两种不同的情况。

1．服务端动态 Web 页面的生成

实际上服务端动态 Web 页面生成最早的可以算是 HTML 表单的处理过程。处理表单和其他交互式 Web 页面的传统方法是一种称为 CGI（公共网关接口）的系统，它是一个标准化的接口，允许 Web 服务器与后端程序及脚本进行通信，这些后端程序和脚本能够接受输入信息，并生成 HTML 页面作为响应。通常，这些后端程序是用 Perl 脚本语言

编写的，习惯上，这些脚本放在 CGI-bin 目录中，用户在 URL 中可以看到这个目录。其原理如图 14-3 所示。

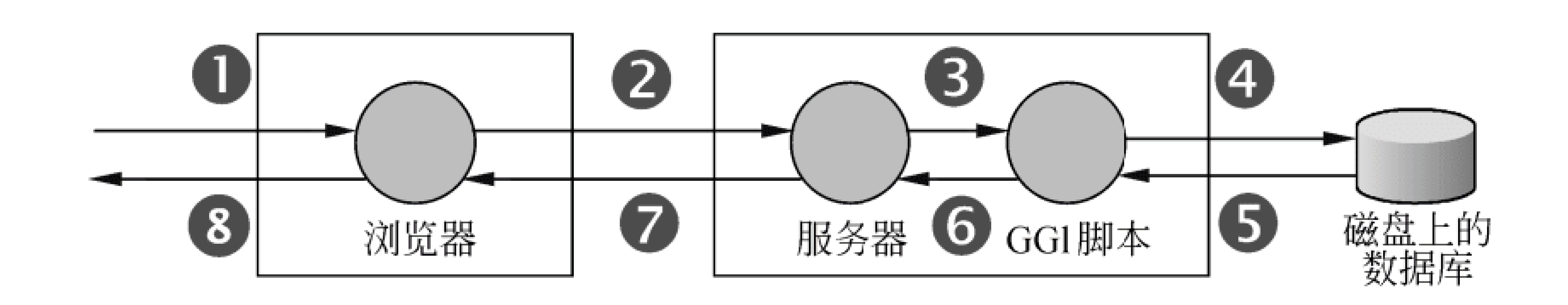


图 14-3　HTML 表单的处理步骤

CGI 脚本可以说是在服务器生成动态内容的第一代方法，第二代方法的特点是在 HTML 页面中嵌入少量的脚本，然后让服务器来执行这些脚本，以便生成最终发送给客户的页面。

其中最流行的包括 PHP，JSP，ASP 三种。PHP 最擅长处理表单，它非常易于使用，实际上是一种面向 Web 和服务器数据库之间的交互过程的功能强大的程序设计语言。它具有变量、字符串、数组，以及在 C 语言中可以找得到的绝大多数控制结构，而且它也有强大的 I/O 功能，从历年考查情况来看，网络管理员并不对它加以考查，只需对它稍微了解。而 JSP 与 PHP 十分相似，只不过页面中动态部分是用 Java 编程语言而非 PHP 来编写，使用这种技术的页面扩展名为 JSP。而 ASP 则是 Microsoft 版本的 PHP 和 JSP，它使用其私有的 VBScript 来生成动态的内容，这种技术的页面文件的扩展名是 ASP。

2．客户端动态 Web 页面的生成

CGI，PHP，JSP 和 ASP 脚本解决了处理表单以及与服务器上的数据库进行交互的问题。但它们无法做响应鼠标移动事件，或者直接与用户交互。为了这个目的，有必要在 HTML 页面中嵌入脚本，而这些脚本则在客户机上被执行，而非在服务器上。在<HTML>中可以使用<Script>标签来使用这样的脚本，最流行的客户端脚本语言是 JavaScript。

JavaScript 是一门全功能的程序设计语言，具有 C 或 Java 的大部分能力，具有变量、字符串、数组、对象、函数和所有常用的控制结构。它还包含大量的专为针对 Web 页面的设施，包括管理窗口和框架的能力、设置和获取 Cookie、处理表单、处理超链接等。在原大纲“网络程序员”的考试中，对 JavaScript 的要求较高，新大纲已将其从考试中去除，因此仅需对其做基本的了解。

而除了 JavaScript 之外，还有另外一种流行的方法，如 Applet。它是被编译成为 JVM 机器指令的 Java 小程序。它可以嵌入到 HTML 页面中去，并被具有 JVM 能力的浏览器解释执行。而 Microsoft 对此的回答是 ActiveX 控件，它是被编译成为 Pentium 机器指令的程序，直接在硬件上执行。

14.3.2 ASP 动态编程

Active Server Pages（ASP）是服务器端脚本编写环境，使用它可以创建和运行动态、交互的 Web 服务器应用程序。使用 ASP 可以组合 HTML 页、脚本命令和 ActiveX 组件以创建交互的 Web 页和基于 Web 的功能强大的应用程序。ASP 应用程序很容易开发和修改。从下面的描述中，我们会发现 ASP 与 JSP 在编程模型和理念方面都十分接近。

1．ASP 模型

浏览器从 Web 服务器上请求 .asp 文件时，ASP 脚本开始运行。然后 Web 服务器调用 ASP，ASP 全面读取请求的文件，执行所有脚本命令，并将 Web 页传送给浏览器。

由于脚本在服务器上而不是在客户端运行，传送到浏览器上的 Web 页是在 Web 服务器上生成的。所以不必担心浏览器能否处理脚本：Web 服务器已经完成了所有脚本的处理，并将标准的 HTML 传输到浏览器。由于只有脚本的结果返回到浏览器，所以服务器端脚本不易复制。用户看不到创建他们正在浏览的页的脚本命令。

2．ASP 的组成

ASP 文件是以.asp 为扩展名的文本文件，这个文本文件可以包括下列部分的任意组合：文本、HTML 标记、ASP 脚本（Script）命令。ASP 脚本是一系列的命令和指令。与 HTML 标签不同，脚本命令指示 Web 服务器执行操作，而 HTML 标签只是简单地格式化文本或读取图形、视频及音频文件。脚本命令可以在变量中存储用户名，在返回到浏览器的页中显示用户名或将用户名存储在数据库中。

脚本命令通过定界符与文本区别开来。定界符是字符或一串字符，它标记单元开始或结束。HTML 使用定界符小于号（<）和大于号（>）插入 HTML 标签。ASP 使用定界符<%和%>插入脚本命令。我们可以在定界符中插入任何命令，只要这些命令对正在使用的脚本语言有效。ASP 中默认的脚本语言是 VBScript，也可以通过设置改为 JavaScript。另外值得一提的是，在 VBScript 中是不区分大小写。但 JavaScript 则是区分大小写的。

3．使用 ASP 的指令

ASP 提供了脚本语言以外的指令。这是一些输出指令和处理指令。

ASP 的输出指令<%= expression %>显示表达式的值。这个输出指令等同于使用 Response.Write 显示信息。例如，输出表达式 <%= sport %> 将文字 climbing（变量当前的值）传送到浏览器。

ASP 处理指令<%@ keyword %>为 ASP 提供处理.asp 文件所需的信息。例如，下面的指令将 VBScript 设为该页的主脚本语言：

```
<%@ LANGUAGE=VBScript %>
```

4．使用变量

变量是计算机内存中已命名的存储位置，其中包含了数字或字符串等数据。变量包含的信息被称为变量的值。变量使用户便于理解脚本操作的名称为用户提供了一种存储、检索和操作数据的途径。

对于 VBScript 而言，并不需要声明变量，但在使用所有变量前声明它们是一种好的脚本书写习惯。要在 VBScript 中声明变量，要使用 Dim、Public 或 Private 语句。例如：

```
<% Dim UserName %>
```

对 Microsoft Jscript 而言仅当变量为本地过程变量时才需声明，但在使用所有变量前声明它们是一种好的脚本书写习惯。要声明一个变量，则使用 var 语句。例如：

```
<% var UserName; %>
```

变量的作用域即生命期，决定哪些脚本命令可访问变量。在过程内部声明的变量具有局部作用域。每执行一次过程，变量就被创建然后消亡。而过程外部的任何命令都不能访问它。在过程外部声明的变量具有全局作用域，其值能被 ASP 页上的任何脚本命令访问和修改。

5．使用集合

大多数 ASP 内建对象支持集合。集合是存储字符串、数字、对象和其他值的地方。除了在存储或取出项目时集合会自动扩展与搜索外，集合与数组非常相近。与数组不同的是，集合被修改后，项目的位置将会移动。可以通过集合中项目的名称、索引或者通过在集合的所有项目中遍历访问项目。

通过使用项目名称可以访问集合中的具体项目。例如，Contents 集合拥有在 Session 对象中保存的所有变量。同样也拥有由 Server.CreateObject 创建的所有对象。假设在 Session 对象中存储了下列用户信息：

```
<%
Session.Contents(\"FirstName\") = \"Sam\"
Session.Contents(\"LastName\") = \"Woo\"
Session.Contents(\"Age\") = 29
%>
```

可以使用在集合中存储项目时关联的名称访问项目。例如，下面的表达式返回字符串"Sam\"：

```
<%= Session.Contents(\"FirstName\") %>
```

通过使用与项目关联的索引或号码也可以访问项目。例如，下面的表达式检索存储在 Session 对象的第二个存储槽中的信息并且返回\"Woo\"：

```
<%= Session.Contents(2) %>
```

ASP 集合从 1 开始编号。当在集合中增加或删除项目时，与项目关联的索引将会改变。

可以使用 VBScript 中的 For...Next 语句遍历集合。例如，要列出上例中存储在 Session 中的三个项目，可以使用下列语句。

```
<%
    Dim Item
    For Item = 1 to 3
    Response.Write Session.Contents(Item) & \"<BR>\"
    Next
%>
```

6. ASP 内建对象

ASP 提供内建对象，这些对象使用户更容易收集通过浏览器请求发送的信息、响应浏览器，以及存储用户信息。

Application 对象：可以使用 Application 对象使给定应用程序的所有用户共享信息。

Request 对象：可以使用 Request 对象访问任何用 HTTP 请求传递的信息，包括从表单用 POST 方法或 GET 方法传递的参数、cookie 和用户认证。Request 对象使您能够访问发送给服务器的二进制数据，如上载的文件。

Response 对象：可以使用 Response 对象控制发送给用户的信息。包括直接发送信息给浏览器、重定向浏览器到另一个 URL 或设置 cookie 的值。

Server 对象：Server 对象提供对服务器上的方法和属性进行的访问。最常用的方法是创建 ActiveX 组件的实例（Server.CreateObject）。其他方法用于将 URL 或 HTML 编码成字符串，将虚拟路径映射到物理路径以及设置脚本的超时期限。

Session 对象：可以使用 Session 对象存储特定的用户会话所需的信息。当用户在应用程序的页之间跳转时，存储在 Session 对象中的变量不会清除；而用户在应用程序中访问页时，这些变量始终存在。也可以使用 Session 方法显式地结束一个会话和设置空闲会话的超时期限。

ObjectContext 对象：可以使用 ObjectContext 对象提交或撤销由 ASP 脚本初始化的事务。

7. ASP 数据库操作

一般来说，一个真正的、完整的站点是离不开数据库的，因为实际应用中，需要保存的数据很多，而且这些数据之间往往还有关联，利用数据库来管理这些数据，可以很方便地查询和更新。数据库有很多种，如 Fox 数据库（.dbf）、Access 数据库（.mdb）、Oracle 和 SQL Server 等，这里以 Microsoft Access 数据库为例来说明 ASP 是如何访问

数据库的。

常用数据库语句如下：

SELECT 语句：命令数据库引擎从数据库里返回信息，作为一组记录。

INSERT INTO 语句：添加一个或多个记录至一个表。

UPDATE 语句：创建更新查询来改变基于特定准则的指定表中的字段值。

DELETE 语句：创建一个删除查询把记录从 FROM 子句列出并符合 WHERE 子句的一个或更多的表中清除。

EXECUTE 语句：用于激活 PROCEDURE（过程）。

1）建立数据库

用 Microsoft Access 建立一个名为 data.mdb 的空数据库，使用设计器创建一个新表，如表 14-28 所示。

保存为 data.mdb 文件，为了便于说明，只是做了一个比较简单的表。

表 14-28　DATA 表结构

字 段 名 称	数 据 类 型	说　明	其　他
ID	自动编号	数据标识	字段大小：长整型 新值：递增　索引：有
username	文本	姓名	缺省值
usermail	文本	E-mail	缺省值
view	数字	查看次数	字段大小：长整型　默认值：0　索引：无
indate	时间日期	加入时间	缺省值

2）连接数据库

方法 1：

```
Set conn = Server.CreateObject("ADODB.Connection")
conn.Open "driver={Microsoft Access Driver (*.mdb)};dbq="&Server.MapPath
("data.mdb")
```

方法 2：

```
Set conn = Server.CreateObject("ADODB.Connection")
conn.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source="&Server.Map-
Path("data.mdb")
```

注意：一个页面中，只要连接一次就可以了，数据库使用完后要及时关闭连接。

```
conn.Close
Set conn = Nothing
```

3）添加新记录到数据库

```
Set conn = Server.CreateObject("ADODB.Connection")
conn.Open "driver={Microsoft Access Driver (*.mdb)};dbq="&Server.MapPath
("data.mdb")
username = "tangles"
usermail = tangles@csai.cn
indate = Now()
sql = "insert into data (username,usermail,indata)
values('"&username&"','"&usermail&"','"&indate&"')"
conn.Execute(sql)
conn.Close
Set conn = Nothing
```

说明：建立数据库连接；通过表单获取姓名、E-mail 字符串，Now()获取当前时间日期；使用 insert into 语句添加新记录；conn.Execute 来执行；最后关闭连接。

4）选择数据库里的记录

选择所有记录的字段（按记录倒序排序）：

```
sql = "select * from data order by ID desc"
```

选择所有记录的姓名和 E-mail 字段（不排序）：

```
sql = "select username,usermail from data"
```

选择姓名为“tangles”的所有记录：

```
sql = "select * from data where username='"tangles"'"
```

选择使用希赛信箱的所有记录（按查看次数排序）：

```
sql = "select * from data where usermail like '%"@csai.cn"%' order by view
desc"
```

选择最新的 10 个记录：

```
sql = "select top 10 * from data order by ID desc"
```

SQL 语句与数据库查询在前面章节中已有介绍，但在 Web 应用时，还得创建一个 RecordSet 对象得到记录集，才能把从数据库里取出的值应用在网页上，如果现在将所有的记录显示在网页上就这样：

```
Set conn = Server.CreateObject("ADODB.Connection")
```

```
conn.Open "driver={Microsoft Access Driver (*.mdb)};dbq="&Server.
MapPath("data.mdb")
sql = "select * from data"
Set rs = Server.CreateObject("ADODB.RecordSet")
rs.Open sql,conn,1,1
Do While Not rs.Eof
Response.Write "<p>姓名："& rs("username") &" E-mail："& rs("usermail")
&" 查看："& rs("view") &"次 "& rs("indate") &"加入</p>"
rs.MoveNext
Loop
rs.Close
Set rs = Nothing
conn.Close
Set conn = Nothing
```

说明：建立数据库连接；创建 rs 得到记录集；循环显示记录，rs.Eof 表示记录末尾，rs.MoveNext 表示移到下一个记录；最后关闭。

5）修改（更新）数据库记录（修改记录的 E-mail）

```
Set conn = Server.CreateObject("ADODB.Connection")
conn.Open "driver={Microsoft Access Driver (*.mdb)};dbq="&Server.MapPath
("data.mdb")
ID = 1
    usermail = "tangle@csai.cn"
    sql = "update data set usermail='"&usermail&"' where ID="&CInt(ID)
    conn.Execute(sql)
    conn.Close
    Set conn = Nothing
```

说明：建立数据库连接；获取记录 ID、新 E-mail 字符串；使用 update 语句修改记录；conn.Execute 来执行；最后关闭。

如果使记录的查看值加 1，则：

```
t view=view+1 where ID="&CInt(ID)
```

6）删除数据库记录（删除某一条记录）

```
 sql = "update data se
Set conn = Server.CreateObject("ADODB.Connection")
    conn.Open "driver={Microsoft Access Driver (*.mdb)};dbq="&Server.
    MapPath("data.mdb")
```

```
ID = 1
sql = "delete from data where ID="&CInt(ID)
   conn.Execute(sql)
conn.Close
   Set conn = Nothing
```

说明：建立数据库连接；获取记录 ID；使用 delete 语句删除记录；conn.Execute 来执行；最后关闭。

删除多条记录为：

```
sql = "delete from data where ID in (ID1,ID2,ID3)"
```

删除所有记录为：

```
sql = "delete from data"
```

14.3.3 JSP 动态编程

JSP（Java 服务器系统页面）是由 Sun 公司倡导、许多公司参与的一种动态网页技术标准。它是在 Java 平台上用于编写包含诸如 HTML、DHTML、XHTML 和 XML 等含有动态生成内容的 Web 页面的应用程序的技术。JSP 最大的特点就是能够运行在多种操作系统、多种 Web 服务器，实现了跨平台访问。

1．JSP 的三种实现模型

JSP 共有简单模型、Servlet 模型、EJB 模型三种。其中简单模型是指浏览器直接调用 JSP 页面，JSP 页面自己生成被请求的内容（其中有可以使用 JDBC 直接从数据库中获取信息）。JSP 页面能够调用 JDBC 或者 JavaBean 组件来生成结果，并且创建标准的 HTML，然后将结果返回浏览器，整个过程如图 14-4（a）所示。这种模型的优点是编程简单、快速，页面作者可以很容易地根据请求和资源状态生成动态的内容。

第二种模型是基于 Web 的客户机直接对 Servlet 进行请求，由 Server 生成动态的内容，再将结构捆绑到一个结果对象中并且调用 JSP 页面。JSP 页面从该对象中访问动态内容，并将结构发回浏览器，其如图 14-4（b）所示。

第三模型则是将 JSP 作为 EJB 体系结构中的一个中间层次，如图 14-4（c）所示，JSP 页面和后端资源通过 EJB 组件进行交互。

2．一个 JSP 页面的例子

JSP 语法格式与 HTML 十分接近，下面就是一个显示当前系统时间的 JSP 页面实例。

```
<HTML>
<HEAD>
   <TITLE>JSP 页面演示</TITLE>
```

```
</HEAD>
<BODY>
   <P>现在的时间是：
<% java.util.Date date=new java.util.Date();
  out.println(date); %></p>
</BODY>
</HTML>
```

从上面可以看出，JSP 嵌入到 HTML 中的脚本，是包含在“<%”与“%>”之间的。

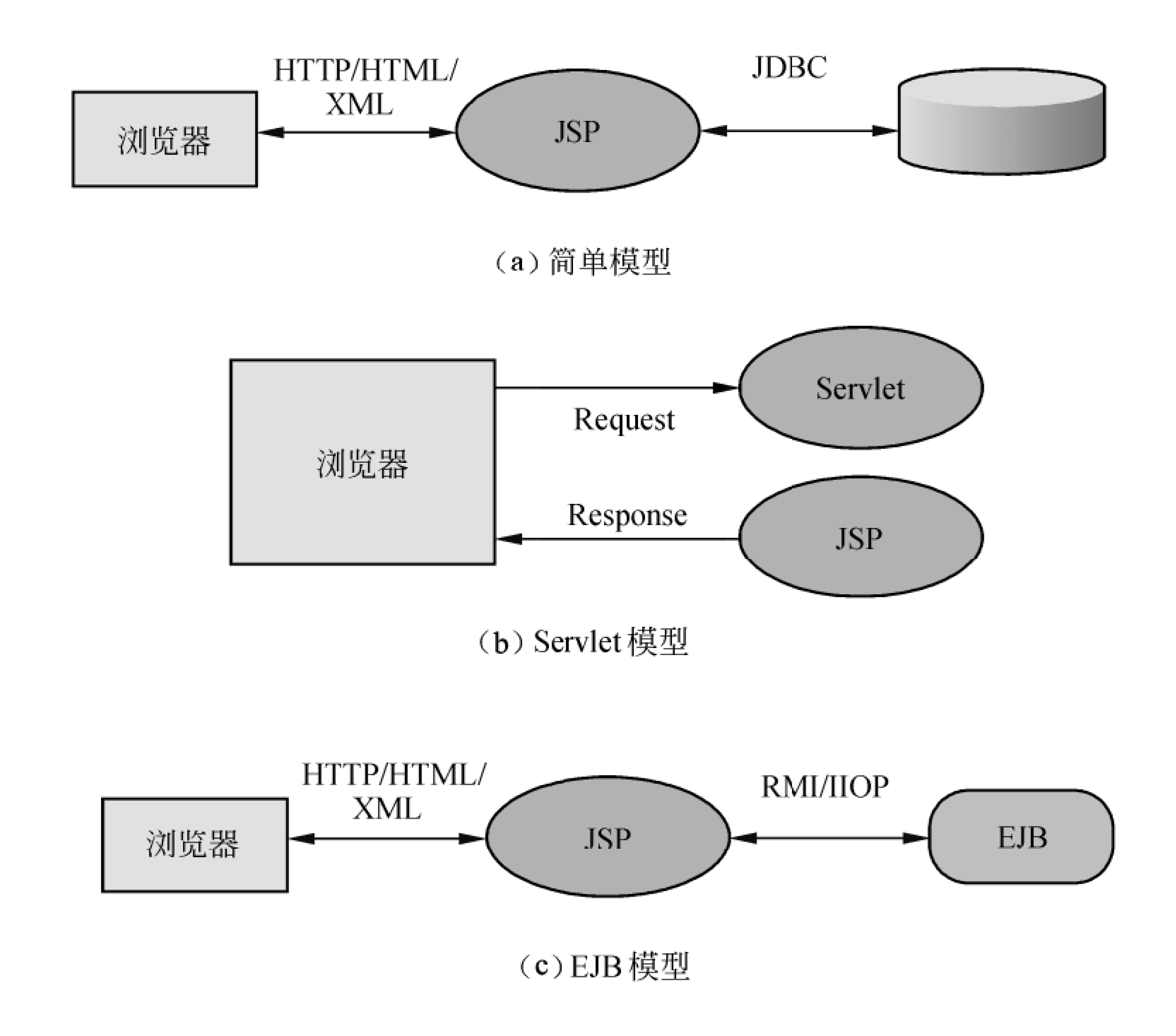


图 14-4　JSP 的三种实现模型

3．JSP 语法基础

JSP 元素共包括指令元素、脚本元素和动作元素三种类型。JSP 中的元素可以是指令或者是动作。在指令中可以提供一些全局的信息，理论上完全独立于 JSP 页面所接收到的任何特定的请求。而动作则是为并发请求处理阶段提供的信息。在一个动作中可以创建一些对象，并通过一些特定的脚本变量使其成为可被利用的脚本元素。

（1）指令类语法：在 JSP 中主要包括 page、include、taglib 三个指令。其中 page 指令用来向 JSP 页面传递与页面相关的信息。其包括的属性如表 14-29 所示。

而 include 指令则是用来指定 JSP 翻译时要插入的文本或代码。包含的过程是静态的，也就是将所包含的文件的文本直接加入到 JSP 文件中。

在 JSP 引擎中有一套重要的标记，可以被扩展到包含带有它们自己的语义的定制的标记中。这个集合称为“标记库”。

表 14-29 page 指令的主要属性

属　　性	属 性 说 明
language	定义了在翻译单元中的 Scriptlet、表示式和声明中使用的脚本语言
extends	定义 JSP 的超类的名字
import	描述了脚本环境中可以使用的类型
session	设置该页面是否要加入到一个 session，默认值是“true”
buffer	设置缓冲区大小，none 表示没有
autoFlush	说明当缓冲区占满时，输出流是否自动刷新，默认为 true，若为 false 则抛出异常
isThreadSafe	说明了实现页面的线程的安全性，若为 true 则将多个客户请求同时分派给页面
isErrorPage	说明当前 JSP 页面是否为另一个 JSP 页面的错误显示页面的 URL 目标
errorPage	是一个以“URL 路径”来描述的 JSP 页面
contentType	定义 JSP 页面及其相应的字符编码

而声明 JSP 页面中使用定制的标记需使用 taglib 指令，该指令的语法为：

```
<%@ taglib uri=" tagLibraryURI" prefix=" tagPrefix" %>
uri：定义统一资源的标记符
prefix：定义在定制的标记名字之前的前缀
```

（2）动作类语法：绝大多数的 JSP 处理要通过 JSP 中的动作元素来完成，动作元素可能会影响输出流和对象的使用、修改或者创建。常见的动作如表 14-30 所示。

表 14-30 JSP 主要动作

动　　作	说　　明
<jsp:useBean>	在 JSP 页面中声明一个 JavaBean 组件实例
<jsp:setProperty>	用来在一个 Bean 中设置性质的值
<jsp:getProperty>	把 Bean 实例的性质的值转换为字符串，置入隐含的输出对象中
<jsp:include>	可以包含与当前页面相同的静态和动态的资源
<jsp:forward>	把传送到一个 JSP 文件的请求对象转而传送到另一个文件处理
<jsp:plugin>	生成一些包含了依赖客户浏览器的结构，并作为 Java 插件下载

（3）脚本语法：JSP 脚本元素提供了把 Java 代码插入由当前的 JSP 页面产生的 Servlet 中的功能。在 JSP 中主要有三种脚本语言元素，如表 14-31 所示。

表 14-31　JSP 脚本

脚 本 类 型	说　　明	语　　法
声明	声明一些变量和方法	<%! declaration(s) %>　例如：<%! int i=0; %>， <%! Public void f(int i){if (i<3) out.println("…");} %>
小脚本	任意长度的脚本片断	<% scriptlet %>
表达式	需要计算的脚本语言表达式	<%= expression %>　例如：<%= a+b+c %>， <%= new java.util.Date() %>

14.4　例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 5 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

下面程序在 IE 浏览器中的显示结果为（1）。

```
<html>
<head><meta>我的网站</meta></head>
<body>主题</body>
</html>
```

（1）A．我的网站　　B．主题
　　C．什么也不显示　　D．显示出错

例题 1 分析

<html></html>：向浏览器表明此文档为超文本文档。

<head></head>：文档头，包含一些初始化信息，包括 title，JavaScript 等。

<body></body>：文档体，包含 HTML 文档的具体内容，也是浏览器所显示的内容。

<meta.../>：该标记不成对出现，它记录了 HTML 的额外信息描述，不显示在页面中。

例题 1 答案

（1）B

例题 2

在超文本中插入视频剪辑文件 sample4.avi，鼠标移到 AVI 播放区域上时，才开始播放 AVI。实现这一功能正确的 HTML 程序为（2）。

（2）A．＜IMG dynsrc＝"sample4.htm" start＝fileopen＞
　　B．＜IMG dynsrc＝"sample4.gif" start＝fileopen＞
　　C．＜IMG dynsrc"sample4.avi" start＝mouseover＞

D．＜IMG dynsrc＝"sample4.gif" start＝mouseover＞

例题 2 分析

文件名应指定为 sample4.avi。

Start 标识应为 mouseover，鼠标移动到该区域上时，播放视频。

例题 2 答案

（2）C

例题 3

采用 HTML 创建一个 E-mail 地址的链接，下面正确的句法是 （3） 。

（3）A．和我联系

B．和我联系

C．和我联系

D．和我联系

例题 3 分析

Mailto 协议（Mailto Protocol）：电子邮件协议。通过该协议可以创建一个指向电子邮件地址的超级链接，通过该链接可以在 Internet 中发送电子邮件。

应用：

比如在网页代码中插入一段 A href="mailto:abc@xxx.com"，那么单击该超链接就会打开 OE 等邮件客户端程序，输入相应的内容后就可以向abc@xxx.com发送邮件。另外，在 IE 浏览器的地址栏中输入 mailto:abc@xxx.com，回车后同样可以达到这样的效果。

例题 3 答案

（3）A

例题 4

ASP 提供的内嵌对象中， （4） 对象的值只能在一个会话的生命期中使用。

（4）A．Session　B．Application　C．Request　D．Server

例题 4 分析

Request 对象为脚本提供客户端在请求一个页面或传送一个窗体时提供的所有信息，这包括能够标识浏览器和用户的 HTTP 变量及附在 URL 后面的值。

Application 对象是在为响应一个 ASP 页的首次请求而载入 ASP DLL 创建的。它提供了存储空间用来存放变量和对象的引用，可用于所有的页面，任何访问者都可以打开，它的生命周期在 Web 服务开始到结束。

Session 对象是在首次请求一个 ASP 页时创建的，它只能供目前的访问者在会话的生命周期中打开的页面使用。

Server 对象提供了一系列的方法和属性，在使用 ASP 编写脚本时是非常有用的。

例题 4 答案

（4）A

例题 5

以下是用 ASP 实现的一个在线留言系统。用 IE 打开网页文件“index.html”后的效果如图 14-5 所示。



图 14-5　显示效果

【index.html 文档的内容】

```
<html>
<head>
<title>在线留言系统</title>
</head>
<body>
<p align="center"><font color="#006699">在 线 留 言 系 统</font></p>
<form method="post" action="submit.asp">
<table border="0" cellspacing="1" width="89%">
<tr>
<td>姓名： </td>
<td><__(2)__name="name" size="30" class="text" maxlength="20"></td>
</tr>
<tr>
<td>性别：</td>
<td><__(3)__name="sex" size="1">
   <option selected>请选择你的性别</option>
   <option value="男">男</option>
   <option value="女">女</option>
   </select></td>
</tr>
```

```
<tr>
<td><b>简短留言：</font></b></td>
<td><(4) name="content" rows="6" cols="45" class="text"></textarea></td>
</tr>
<tr>
<td>< (5) name="submit" class="btn" value="提交留言"></td>
<td>< (6) name="B1" value="全部重填" class="btn"></td>
</tr>
</table>
</form>
</body>
</html>
```

【submit.asp 文档的内容】

```
<%
If request.form("name")="" Then
response.write"<script>alert('请填写留言人姓名!'); history.back()</script>"
response.end
End If
If request.form("sex")="" or  request.form("sex")="请选择你的性别" Then
response.write"<script>alert('请选择留言人性别');history.back()</script>"
response.end
End If
If len( (7) )>100 Then
response.write"<script>alert('留言不能超过100字! ');history.back()</script>"
response.end
End If
%>
<!--#include file="conn.asp"-->
<%
dim rs,sql
set rs=server. (8)
sql="select * from data where (id is null) "
rs.open sql,conn,1,3
rs. (9)
rs("name")= (10)
rs("sex")=request.form("sex")
rs("content")=request.form("content")
rs("date")=now()
rs("ip")=request.ServerVariables("remote_addr")
```

```
rs.  (11)  
rs.close
conn.close
response.redirect"success.asp"
%>
```

【问题 1】

将以上 index.html 更名为 （1） 后，将不能直接在 IE 中正常显示该网页。

（1）A．index.htm　　B．index.php　　C．index.asp

【问题 2】

为 index.html 文件中的（2）～（6）处空缺选择正确答案。

（2）～（6）备选答案：

A．input type="reset"　　B．input type="submit"　　C．input type="text"

D．textarea　　E．option　　F．select　　G．radio

【问题 3】

从以下备选答案中为 submit.asp 程序中（7）～（11）处空缺选择正确答案。

（7）A．request.querystring("content")
　　B．request.querystring ("name")
　　C．request.form("content")
　　D．request.form("name")

（8）A．mappath("adodb.recordset")
　　B．createobject("adodb.recordset")
　　C．new("adodb.recordset")
　　D．htmlencode("adodb.recordset")

（9）A．addnew　　B．add　　C．eof　　D．insert

（10）A. request.querystring("content")　　B．request.querystring ("name")
　　C．request.form("content")　　D．request.form("name")

（11）A．submit　　B．update　　C．append　　D．refresh

【问题 4】

response.redirect"success.asp" 语句的作用是 （12） 。

（12）A．弹出 success.asp 网页窗口
　　B．重定向到 success.asp 网页
　　C．关闭 success.asp 程序
　　D．修改 success.asp 程序

例题 5 分析

【问题 1】

本题考查 Web 站点设置中默认文档的设置操作。如图 14-6 所示，当启用默认文档

后，服务器端会按以上优先级提供给客户端的 Web 请求。

容易发现：A. index.htm 和 C. index.asp 都包括在该列表中，当将 index.html 更名为以上任意文件时，均可以正常访问默认页面，而 index.php 却不能正常访问，若要正常访问，需执行“添加”命令将该页面项添加进去。

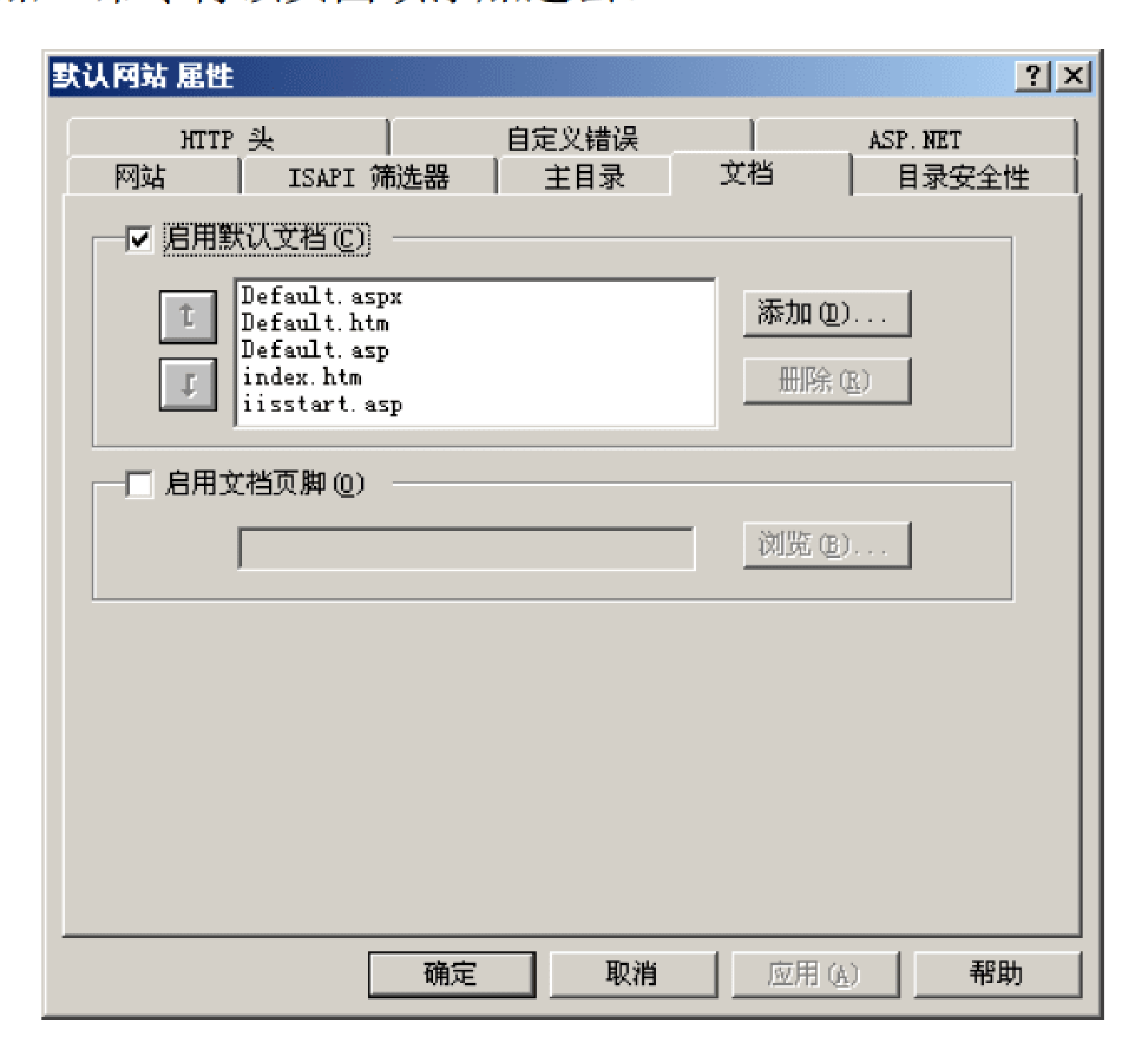


图 14-6 设置界面图

【问题 2】

本题 HTML 表单的相关知识。利用<INPUT>字段的各个属性可以生成其他类型的输入字段，表 14-32 列出了最常用的输入字段标志和属性。

表 14-32 输入字段标志与属性

属性/标志	说　　明
<INPUT>	在表单中设置访问者输入的区域
TYPE="…"	设置输入字段的类型，可以取值 TEXT（文本）、PASSWORD（密码）、CHECKBOX（复选框）、RADIO（单选项）、FILE（文件）、HIDDEN（隐藏字段）、IMAGE（图像）、SUBMIT（提交按钮）、RESET（复位按钮）
NAME="…"	处理表单结果
VALUE="…"	提供与 NAME 相关联的内容，该属性用于复选框和单选按钮，因为它们不接受其他输入，可用此属性用于文本字段，提供初始输入
SIZE="n"	设置字段的显示长度，这个属性用于文本输入字段
MAXLENGTH="n"	设置可提交的最长的字符集，这个属性用于文本字段
ACCEPT="…"	设置可接受的上传文件的 MIME 类型，可用通配符

下面就以文本字段为例来说明。文本字段是表单中的空白区，用来供访问者输入信息，图 14-7 就是一个使用文本字段的实例。

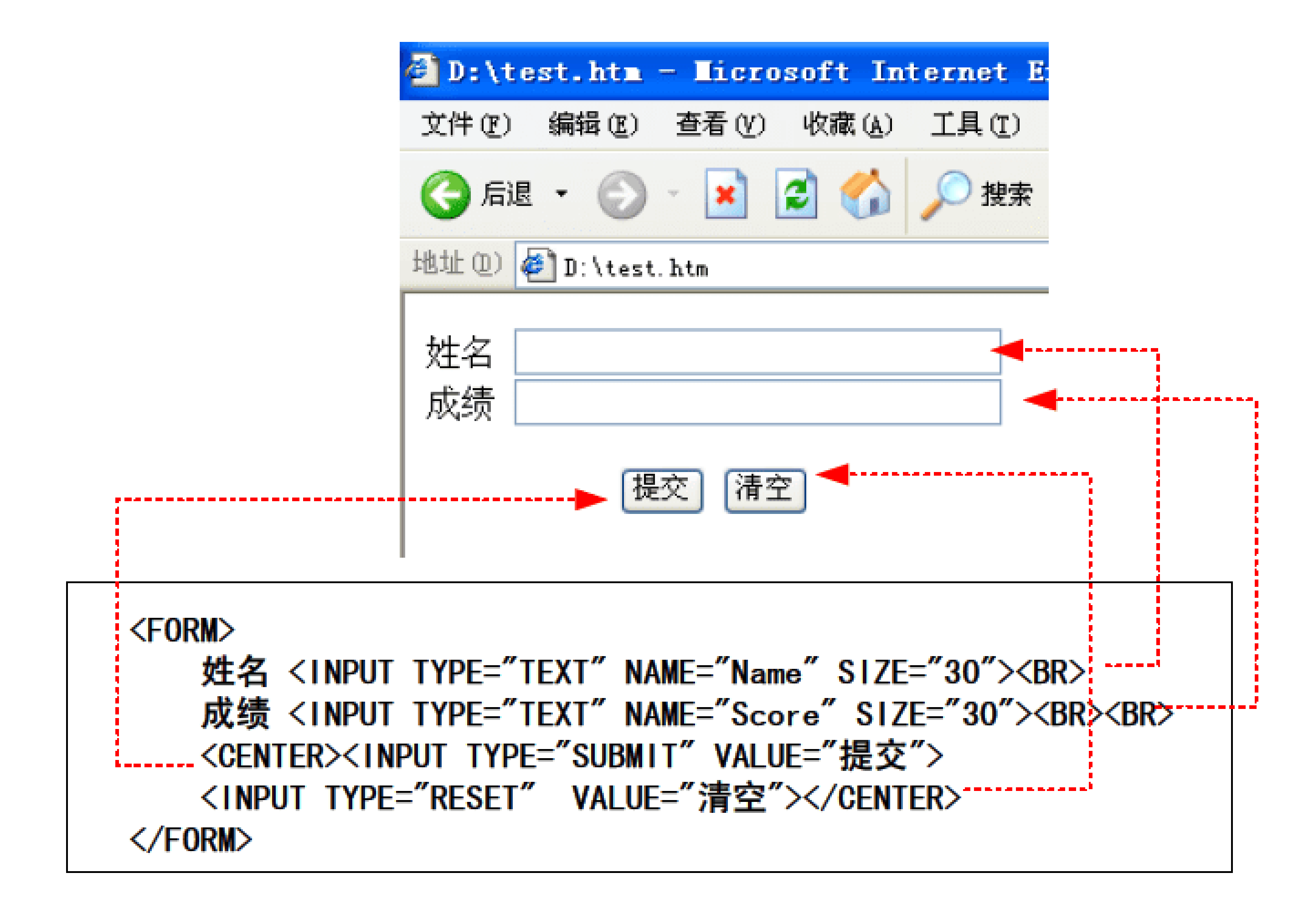


图 14-7　文本字段示例

从效果图与程序中很容易读出：（2）处是单行文本框，input type="text"（4）处是多行文本框，input type="stextarea"（5）处是表单提交按钮，input type="submit"（6）处是重置按钮，input type="reset"。而（3）处是一个下拉列表框，这里应填入“select”。具体属性及字段标志如表 14-33 所示。

表 14-33　属性及字段标志

属性/标志	说　明
<SELECT>	在表单中设置选择字段区，样子像个下拉清单或选择字段
NAME="…"	建立输入字段下标题，NAME 属性用于表单处理
SIZE="n"	设置选择字段下拉清单的显示尺寸，默认为 1，如果要显示多个选项，可以修改值
MULTIPLE	将选择字段设置为接受多个选项，这个属性和 SIZE 属性一起设置最大选项数
<OPTION>	标识选择字段中包括的项目，每个项目都要用一个<OPTION>标志
VALUE="…"	提供与 NAME 属性相关联的内容
SELELTED	可以指定默认选项，在表单装入或复位时显示

【问题 3】

request.form("content")：Request.Form()即获取以 POST 方式提交的数据（接收 Form 提交来的数据），"content"参数指名称为 content 的 text area 控件。

set rs=server. createobject("adodb.recordset")：该命令指创建一个名为 rs 的记录集对象 adodb.recordset。用于存放数据库信息。

rs. Addnew：记录集中添加一条新记录，便于存放新录入的数据。

rs("name")= request.form("name")：将从 Form 获取来的 name 信息暂时存入新插入记录的 name 字段。

rs. Update：将记录集中存储的信息保存更新到数据库中。

【问题 4】

这里简单介绍一下 ASP 动态网页编程中两种跳转语句的区别：

Response.Redirect：发送一个 HTTP 响应到客户端，告诉客户端跳转到一个新的页面，客户端再发送跳转请求到服务器。使用此方法时，将无法保存所有的内部控件数据，页面 A 跳转到页面 B，页面 B 将无法访问页面 A 中 Form 提交的数据。

Server.Transfer：用于把处理的控制权从一个页面转移到另一个页面，在转移的过程中，没有离开服务器，内部控件（如 request，session 等）的保存的信息不变，因此，你能从页面 A 跳到页面 B 而不会丢失页面 A 中收集的用户提交信息。此外，在转移的过程中，浏览器的 URL 栏不变。

例题 5 答案

【问题 1】

（1）B

【问题 2】

（2）C　（3）F　（4）D　（5）B　（6）A

【问题 3】

（7）C　（8）B　（9）A　（10）D　（11）B

【问题 4】

（12）B

第 15 章　网络安全技术

根据网络管理员的考试大纲要求，本章应掌握防火墙技术、入侵检测技术、信息加密与认证技术、密钥管理与数字证书及一些常见的安全协议 SSL/SET、SHTTP、PGP 等相关知识。

15.1　防火墙技术

防火墙（FireWall）成为近年来新兴的保护计算机网络安全技术性措施。它是一种隔离控制技术，在不同网域之间设置屏障，阻止对信息资源的非法访问，也可以使用防火墙阻止重要信息从企业的网络上被非法输出。

作为 Internet 网的安全性保护软件，FireWall 已经得到广泛的应用。通常企业为了维护内部的信息系统安全，在企业网和 Internet 间设立 FireWall 软件。企业信息系统对于来自 Internet 的访问，采取有选择的接收方式。它可以允许或禁止一类具体的 IP 地址访问，也可以接收或拒绝 TCP/IP 上的某一类具体的应用。

15.1.1　防火墙的概念

防火墙是位于两个或多个网络之间，执行访问控制策略的一个或一组系统，是一类防范措施的总称。防火墙的作用是防止不希望的、未经授权的通信进出被保护的网络，通过边界控制强化内部网络的安全政策。防火墙通常放置在外部网络和内部网络的中间，执行网络边界的过滤封锁机制，如图 15-1 所示。

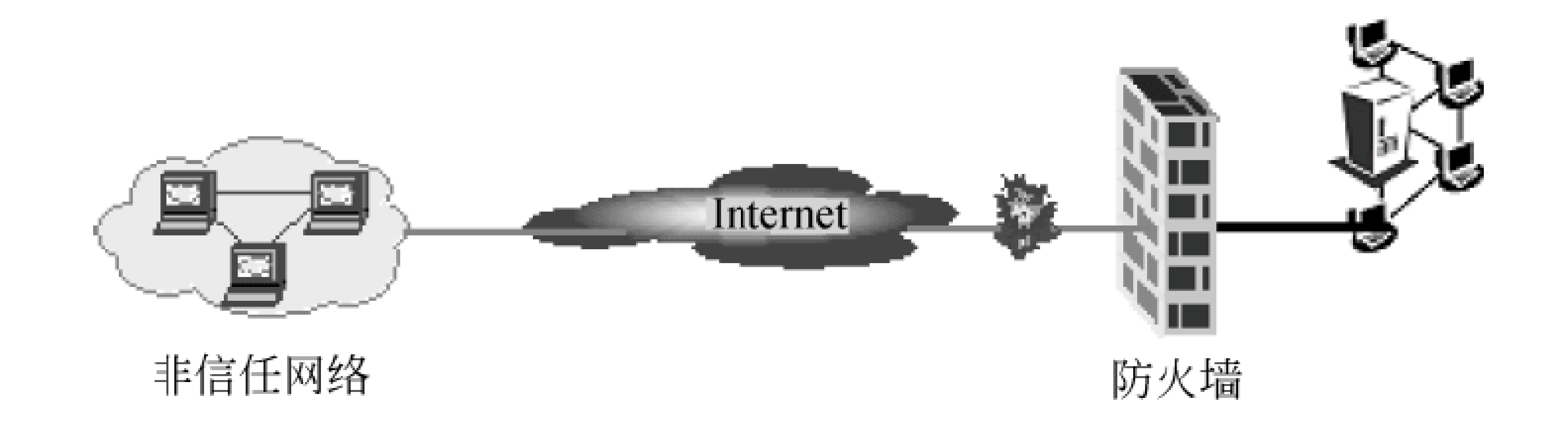


图 15-1　防火墙的位置

防火墙通常是运行在一台或者多台计算机上的一组特别的服务软件，用于对网络进行防护和通信控制。但是在很多情况下防火墙以专门的硬件形式出现，这种硬件也被称为防火墙，它是安装了防火墙的软件，并针对安全防护进行了专门设计的网络设备，本

质上还是软件在进行控制。

如果没有防火墙，整个内部网络的安全性就完全依赖于每个主机，因此，所有的主机在安全水平方面都必须达到一致的高度。也就是说网络的安全水平是由最低的那个安全水平的主机决定的，这就是所谓的“木桶原理”，木桶能装多少水由最低的地方决定。网络越大，对主机进行管理使它们达到统一的安全级别水平就越不容易。

防火墙隔离了内部网络和外部网络，它被设计为只运行专用的访问控制软件的设备，而没有其他的服务，因此也就意味着相对少一些缺陷和安全漏洞。此外防火墙也改进了登录和监测功能，从而可以进行专用的管理。如果采用了防火墙，内部网络中的主机将不再直接暴露给来自 Internet 的攻击。因此对整个内部网络的安全管理就变成了防火墙的安全管理，这样使安全管理变得更为方便和易于控制，也使内部网络更加安全。

防火墙一般放置在被保护网络的边界，必须做到以下几点才能使防火墙起到安全防护的作用：

（1）所有进出被保护网络的通信数据流必须经过防火墙。

（2）所有通过防火墙的通信必须经过安全策略的过滤或者防火墙的授权。

（3）防火墙本身是不可被侵入的。

总之，防火墙是在被保护网络和非信任网络之间进行访问控制的一个或者一组访问控制部件。防火墙是一种逻辑隔离部件，而不是物理隔离部件，它所遵循的原则是在保证网络通畅的情况下，尽可能地保证内部网络的安全。防火墙是在已经制定好的安全策略下进行访问控制，所以一般情况下它是一种静态安全部件，但随着防火墙技术的发展，防火墙通过与入侵检测系统（IDS）进行连动，或者本身集成 IDS 功能，将能够根据实际的情况进行动态的策略调整。

15.1.2 防火墙的功能

防火墙一般具有以下几个功能：

（1）访问控制功能。这是防火墙最基本也是最重要的功能，通过禁止或允许特定用户访问特定的资源，保护网络的内部资源和数据。需要禁止非授权的访问，防火墙需要识别哪个用户可以访问何种资源。它包括了服务控制、方向控制、用户控制、行为控制等功能。

（2）内容控制功能。根据数据内容进行控制，比如防火墙可以从电子邮件中过滤掉垃圾邮件，可以过滤掉内部用户访问外部服务的图片信息，也可以限制外部访问，使它们只能访问本地 Web 服务器中一部分信息。简单的数据包过滤路由器不能实现这样的功能，但是代理服务器和先进的数据包过滤技术可以做到。

（3）全面的日志功能。防火墙的日志功能很重要。防火墙需要完整地记录网络访问情况，包括内外网进出的访问，需要记录访问是什么时候进行了什么操作，以检查网络访问情况。正如银行的录像监视系统一样，记录下整体的营业情况，一旦有什么事情发

生就可以通过录像查明事实。防火墙的日志系统也有类似的作用，一旦网络发生了入侵或者遭到了破坏，就可以对日志进行审计和查询。日志需要有全面的记录和方便的查询功能。

（4）集中管理功能。防火墙是一个安全设备，针对不同的网络情况和安全需要，需要制定不同的安全策略，然后在防火墙上实施，使用中还需要根据情况改变安全策略，而且在一个安全体系中，防火墙可能不止一台，所以防火墙应该是易于集中管理的，这样管理员就可以方便地实施安全策略。

（5）自身的安全和可用性。防火墙要保证自身的安全不被非法侵入，保证正常的工作。如果防火墙被侵入，防火墙的安全策略被修改，这样内部网络就变得不安全。防火墙也要保证可用性，否则网络就会中断，网络连接就会失去意义。

另外防火墙还应带有如下的附加功能：

（1）流量控制，针对不同的用户限制不同的流量，可以合理使用带宽资源。

（2）NAT（Network Address Translation，网络地址转换），是通过修改数据包的源地址（端口）或者目的地址（端口）来达到节省 IP 地址资源，隐藏内部 IP 地址功能的一种技术。

（3）VPN（Virtual Private Network，虚拟专用网），只利用数据封装和加密技术，使本来只能在私有网络上传送的数据能够通过公共网络进行传输，使系统费用大大降低。

15.1.3　防火墙的优点和局限性

防火墙具有以下的优点：

（1）防火墙对企业内部网实现了集中的安全管理，可以强化网络安全策略，比分散的主机管理更经济易行。

（2）防火墙能防止非授权用户进入内部网络。

（3）防火墙可以方便地监视网络的安全性并报警。

（4）可以作为部署网络地址转换的地点，利用 NAT 技术，可以缓解地址空间的短缺，隐藏内部网的结构。

（5）由于所有的访问都经过防火墙，防火墙是审计和记录网络的访问和使用的最佳地方。

然而防火墙的使用也有一定的局限性，列举如下：

（1）为了提高安全性，限制或关闭了一些有用但存在安全缺陷的网络服务，给用户带来了使用上的不便。

（2）目前防火墙对于来自网络内部的攻击还无能为力。

（3）防火墙不能防范不经过防火墙的攻击，如内部网用户通过 SLIP 或 PPP 直接进入 Internet。

（4）防火墙对用户不完全透明，可能带来传输延迟、瓶颈及单点失效。

（5）防火墙不能完全防止受病毒感染的文件或软件的传输，由于病毒的种类繁多，如果要在防火墙完成对所有病毒代码的检查，防火墙的效率就会降到不能忍受的程度。

（6）防火墙不能有效地防范数据驱动式攻击。

（7）作为一种被动的防护手段，防火墙不能阻止因特网不断出现的新的威胁和攻击。

总之，防火墙是解决企业网安全问题的流行方案，即把公共数据和服务置于防火墙外，使其对防火墙内部资源的访问受到限制。作为一种网络安全技术，防火墙具有简单实用的特点，并且透明度高，可以在不修改原有网络应用系统的情况下达到一定的安全要求。

15.1.4 防火墙的分类

防火墙技术一般分为两类：

（1）网络级防火墙：用来防止整个网络出现外来非法的入侵。属于这类的有分组过滤和授权服务器。前者检查所有流入本网络的信息，然后拒绝不符合事先制订好的一套准则的数据，而后者则是检查用户的登录是否合法。

（2）应用级防火墙：从应用程序来进行接入控制。通常使用应用网关或代理服务器来区分各种应用。例如，可以只允许通过访问万维网的应用，而阻止 FTP 应用的通过。

根据不同的应用，对防火墙进行了详细划分，参见表 15-1。

表 15-1 防火墙分类

类　型	特　点	优　点	缺　点
包过滤（访问控制表）	根据定义的过滤规则审查，根据是否匹配来决定是否通过	透明、成本低、速度快、效率高	对 IP 包伪造难以防范、不具备身份认证功能、不能检测高层攻击、过滤多、效率下降快
应用网关	工作在应用层，实现协议过滤和转发功能	能够提供比较成熟的日志功能	速度相对更慢
代理服务	阻断内外网之间的通信，只能够通过“代理”实现	有很高的安全性	速度慢，对用户不透明，协议不同就需要不同的代理，不利于网络新业务
状态检测（自适应/动态包过滤）	通过状态检测技术动态记录、维护各个连接的协议状态	效率很高，动态修改规则可以提高安全性	
自适应代理	根据用户的安全策略，动态适应传输中的分组流量	状态检测+代理	

15.1.5　常见的防火墙技术

防火墙的种类多种多样，在不同的发展阶段，采用的技术也各不相同，采用不同的技术，因而也就产生了不同类型的防火墙。防火墙所采用的技术主要有以下几种。

1．屏蔽路由技术

最简单和最流行的防火墙形式是“屏蔽路由器”。屏蔽路由器采用包过滤或虚电路技术，包过滤通过检查每个 IP 网络包，取得其头信息，一般包括：到达的物理网络接口，源 IP 地址、目标 IP 地址、传输层类型（TCP、UDP、ICMP）、源端口和目的端口。根据这些信息，判别是否与规则集中的某条目匹配，并对匹配包执行规则中指定的动作（禁止或允许）。

2．基于代理的技术

基于代理的防火墙也称应用网关，通常被配置为“双宿主网关”，具有两个网络接口卡，同时接入内部和外部网。由于网关可以与两个网络通信，它是安装传递数据软件的理想位置。代理服务不允许直接与真正的服务通信，而是与代理服务器通信（用户的默认网关指向代理服务器）。各个应用代理在用户和服务之间处理所有的通信。能够对通过它的数据进行详细的审计追踪，许多专家也认为它更加安全，因为代理软件是根据防火墙后面主机的脆弱性来制定的，可以专门防范已知的攻击。

3．包过滤技术

系统按照一定的信息过滤规则，对进出内部网络的信息进行限制，允许授权信息通过，而拒绝非授权信息通过。包过滤防火墙工作在网络层和逻辑链路层之间。截获所有流经的 IP 包，从其 IP 头、传输层协议头，甚至应用层协议数据中获取过滤所需的相关信息。然后依次按顺序与事先设定的访问控制规则进行一一匹配比较，执行其相关的动作。

4．动态防火墙技术

它是针对静态包过滤技术而提出的一项新技术。静态包过滤技术局限于过滤基于源及目的的端口，IP 地址的输入输出业务，因而限制了控制能力。而动态防火墙技术可创建动态的规则，使其适应不断改变的网络业务量。具体地讲，动态防火墙技术并不是根据状态来对包进行有效性检查，而是通过为每个会话维护其状态信息，来提供一种防御措施和方法。

5．DMZ 模型

DMZ 称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。另一方面，通过这样一个 DMZ 区域，更加有效地保护了内部网络，因为这种网络部署，比起

一般的防火墙方案，对攻击者来说又多了一道关卡。网络结构如图 15-2 所示。

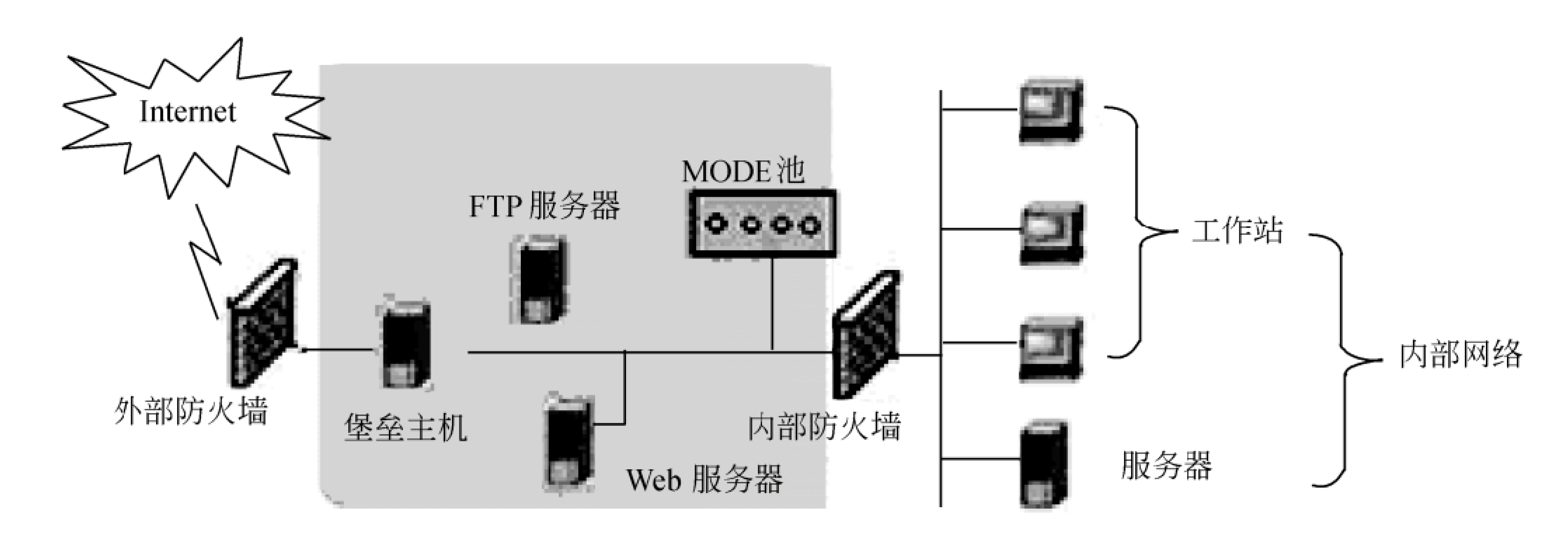


图 15-2 DMZ 模型

在这个防火墙方案中，包括两个防火墙，外部防火墙抵挡外部网络的攻击，并管理所有内部网络对 DMZ 的访问。内部防火墙管理 DMZ 对于内部网络的访问。内部防火墙是内部网络的第三道安全防线（前面有了外部防火墙和堡垒主机），当外部防火墙失效的时候，它还可以起到保护内部网络的功能。而局域网内部，对于 Internet 的访问由内部防火墙和位于 DMZ 的堡垒主机控制。

15.1.6 防火墙配置技术

本知识点重点在于了解 Cisco 防火墙的基本配置方法，了解其最基本的指令。在历年考题中还没有出现过直接相关的题目。

1．防火墙配置基础

在配置 PIX 防火墙之前，先来介绍一下防火墙的物理特性。防火墙通常具有至少两个接口，使用防火墙时，就至少产生了两个网络，描述如下：

- 内部区域（内网）。内部区域通常就是指企业内部网络或者是企业内部网络的一部分。它是互连网络的信任区域，即受到了防火墙的保护。
- 外部区域（外网）。外部区域通常指 Internet 或者非企业内部网络。它是互连网络中不被信任的区域，当外部区域想要访问内部区域的主机和服务，通过防火墙，就可以实现有限制的访问。
- 非军事区（又称停火区）。是一个隔离的网络，或几个网络。位于区域内的主机或服务器被称为堡垒主机。一般在非军事区内可以放置 Web、Mail 服务器等。停火区对于外部用户通常是可以访问的，这种方式让外部用户可以访问企业的公开信息，但却不允许它们访问企业内部网络。

注意：两个接口的防火墙是没有停火区的。

PIX 防火墙提供四种管理访问模式：

- 用户模式：PIX 防火墙开机自检后，就是处于这种模式，系统显示为 pixfirewall> 。

- 特权模式：输入 enable 进入特权模式，可以改变当前配置，显示为 pixfirewall# 。
- 配置模式：输入 config terminal 进入此模式，绝大部分的系统配置都在这里进行，显示为 pixfirewall(config)#。
- 监视模式：PIX 防火墙在开机或重启过程中，按住 Escape 键或发送一个“Break”字符，进入监视模式，这里可以更新操作系统映象和口令恢复。显示为 monitor> 。

Firewall 启用或禁止防火墙的操作如下：

系统默认为禁止防火墙，需使用“firewall”命令来启用或禁止防火墙，可以通过 show firewall 命令看到相应结果。该命令在全局配置模式下配置，它是控制防火墙的总开关。在使用 firewall disable 命令关闭防火墙时，防火墙本身的统计信息也将被清除。命令如下：

firewall　enable | disable

enable、disable 分别表示启用/禁止防火墙。

【举例】 启用防火墙。

Firewall(config)# firewall enable

2．防火墙常规配置

配置 PIX 防火墙有六个基本命令：nameif、interface、ip address、nat、global、route。这些命令在配置 PIX 是必须的。以下是配置的基本步骤：

1）配置防火墙接口的名字，并指定安全级别（nameif）

Pix525(config)# nameif ethernet0 outside security 0

Pix525(config)# nameif ethernet1 inside security 100

Pix525(config)# nameif dmz security 50

注意：在默认配置中，Ethernet0 端口被命名为外部接口（outside），安全级别是 0；Ethernet1 端口被命名为内部接口（inside），安全级别是 100。安全级别取值范围为 1～100，数字越大安全级别越高。若添加新的接口，命令如下：

```
Pix525(config)# nameif pix/intf3 security 40   # 安全级别取值范围在 1～100
```

2）配置以太端口参数（interface）

```
Pix525(config)# interface ethernet0 auto        # auto 选项表明系统自适应网卡
                                                  类型
Pix525(config)# interface ethernet1 100full   # 100full 选项表示 100Mbps
                                                 以太网全双工通信
Pix525(config)# interface ethernet1 100full shutdown    # shutdown 选项表
                              示关闭这个接口，若启用接口去掉 shutdown
```

3）配置内外网卡的 IP 地址（ip address）

```
Pix525(config)# ip address outside 61.144.51.42 255.255.255.248
Pix525(config)# ip address inside 192.168.0.1 255.255.255.0
```

很明显,Pix525 防火墙在外网的 IP 地址是 61.144.51.42,内网 IP 地址是 192.168.0.1 。

3. 网络地址转换

网络地址翻译（NAT）作用是将内网的私有 IP 转换为外网的公有 IP。nat 命令总是与 global 命令一起使用，这是因为 nat 命令可以指定一台主机或一段范围的主机访问外网，访问外网时需要利用 global 所指定的地址池进行对外访问。

1）指定要进行转换的内部地址（nat）

nat 命令配置语法：

```
nat (if_name) nat_id local_ip [netmark]
```

其中参数解释如下：

if_name 表示内网接口名字，例如 inside；

Nat_id 用来标识全局地址池，使它与其相应的 global 命令相匹配；

local_ip 表示内网被分配的 IP 地址，例如 0.0.0.0 表示内网所有主机可以对外访问；

[netmark]表示内网 IP 地址的子网掩码。

例：Pix525(config)# nat（inside）1 0 0

表示启用 nat，应用于全局地址池 1，内网的所有主机都可以访问外网，用 0 可以代表 0.0.0.0 。

例：Pix525(config)# nat（inside） 1 172.16.0.0 255.255.0.0

表示只有 172.16.0.0 这个网段内的主机可以访问外网。

2）指定外部地址范围（global）

global 命令把内网的 IP 地址翻译成外网的 IP 地址或一段地址范围。Global 命令的配置语法：

```
global (if_name) nat_id ip_address-ip_address [netmark global_mask]
```

其中参数解释如下：

if_name 表示外网接口名字，例如 outside；

Nat_id 用来标识全局地址池，使它与其相应的 nat 命令相匹配；

ip_address-ip_address 表示翻译后的单个 IP 地址或一段 IP 地址范围；

[netmark global_mask]表示全局 IP 地址的网络掩码。

例： Pix525(config)# global (outside) 1 61.144.51.42-61.144.51.48

表示内网的主机通过 pix 防火墙要访问外网时，pix 防火墙将使用 61.144.51.42-61.144.51.48 这段 IP 地址池为要访问外网的主机分配一个全局 IP 地址。

例： Pix525(config)# global (outside) 1 61.144.51.42

表示内网要访问外网时，pix 防火墙将为访问外网的所有主机统一使用 61.144.51.42 这个单一 IP 地址。

例：Pix525(config)# no global (outside) 1 61.144.51.42

表示删除这个全局表项。

3）设置指向内网和外网的静态路由（route）

定义一条静态路由。route 命令配置语法：

```
route (if_name) 0 0 gateway_ip [metric]
```

其中参数解释如下：

if_name 表示接口名字，例如 inside，outside；

Gateway_ip 表示网关路由器的 IP 地址；

[metric]表示到 gateway_ip 的跳数，通常默认是 1。

例：Pix525(config)# route outside 0 0 61.144.51.168 1

表示一条指向边界路由器（IP 地址 61.144.51.168）的默认路由。

例：Pix525(config)# route inside 10.1.1.0 255.255.255.0 172.16.0.1 1

Pix525(config)# route inside 10.2.0.0 255.255.0.0 172.16.0.1 1

如果内部网络只有一个网段，按照上例设置一条默认路由即可；如果内部存在多个网络，需要配置一条以上的静态路由。上面那条命令表示创建了一条到网络 10.1.1.0 的静态路由，静态路由的下一条路由器 IP 地址是 172.16.0.1。

4）配置静态 IP 地址翻译（static）

如果从外网发起一个会话，会话的目的地址是一个内网的 IP 地址，static 就把内部地址翻译成一个指定的全局地址，允许这个会话建立。

static 命令配置语法：

```
static (internal_if_nameexternal_if_name) outside_ip_address inside_
ip_address
```

其中参数解释如下：

internal_if_name 表示内部网络接口，安全级别较高，如 inside；

external_if_name 为外部网络接口，安全级别较低，如 outside 等；

outside_ip_address 为正在访问的较低安全级别的接口上的 IP 地址；

inside_ ip_address 为内部网络的本地 IP 地址。

例：Pix525(config)# static (inside, outside) 61.144.51.62 192.168.0.8

表示 IP 地址为 192.168.0.8 的主机，对于通过 pix 防火墙建立的每个会话，都被翻译成 61.144.51.62 这个全局地址，也可以理解成 static 命令创建了内部 IP 地址 192.168.0.8 和外部 IP 地址 61.144.51.62 之间的静态映射。

例： Pix525(config)# static (inside, outside) 192.168.0.2 10.0.1.3

Pix525(config)# static (dmz, outside) 211.48.16.2 172.16.10.8

注释同上例。通过以上几个例子说明使用 static 命令可以让我们为一个特定的内部 IP 地址设置一个永久的全局 IP 地址。这样就能够为具有较低安全级别的指定接口创建一个入口，使它们可以进入到具有较高安全级别的指定接口。

4．访问控制技术

1）firewall default 命令

firewall default 用于配置防火墙在没有相应的访问规则匹配时，默认的过滤方式。当在接口应用的规则没有一个能够判断一个报文是否应该被允许还是禁止时，默认的过滤属性将起作用；如果默认过滤属性是“允许”，则报文可以通过，否则报文被丢弃。在防火墙开启的情况下，报文被默认允许通过。

该命令在全局配置模式下配置，命令格式为：

```
firewall default { permit | deny }
```

【参数说明】

permit 表示默认过滤属性设置为“允许”。

deny 表示默认过滤属性设置为“禁止”。

例：设置默认过滤属性为“允许”。

```
Quidway(config)#firewall default permit
```

2）ip access-group 命令

使用此命令将规则应用到接口上，使用此命令的 no 形式来删除相应的设置，与之相关的命令如前面提到过的 access-list。在默认情况下，没有规则应用于接口。

使用此命令来将规则应用到接口上；如果要过滤从接口收上来的报文，则使用 in 关键字；如果要过滤从接口转发的报文，使用 out 关键字。一个接口的一个方向上最多可以应用 20 类不同的规则；这些规则之间按照规则序号的大小进行排列，序号大的排在前面，也就是优先级高。对报文进行过滤时，将采用发现符合的规则即得出过滤结果的方法来加快过滤速度。所以，建议在配置规则时，尽量将对同一个网络配置的规则放在同一个序号的访问列表中；在同一个序号的访问列表中，规则之间的排列和选择顺序可以用 show access-list 命令来查看。

该命令在接口配置模式下配置，命令格式为：

```
ip access-group listnumber { in | out }
[ no ] ip access-group listnumber { in | out }
```

【参数说明】

listnumber 为规则序号，是 1～199 之间的一个数值。

in 表示规则用于过滤从接口收上来的报文。

out 表示规则用于过滤从接口转发的报文。

例：将规则 101 应用于过滤从以太网口收上来的报文。

```
Quidway(config-if-Ethernet0)#ip access-group 101 in
```

3）settr 命令

Settr：设定或取消特殊时间段。使用此命令来设置时间段；可以最多同时设置 6 个时间段，通过 show timerange 命令可以看到所设置的时间。如果在已经使用了一个时间段的情况下改变时间段，则此修改将在一分钟左右生效（系统查询时间段的时间间隔），设置的时间应该是 24 小时制。系统默认没有设置时间段，即认为全部为普通时间段。

该命令在全局配置模式下配置，命令格式为：

```
settr begin-time end-time
no settr
```

【参数说明】

begin-time 为一个时间段的开始时间。

end-time 为一个时间段的结束时间，应该大于开始时间。

例：设置时间段为 8:30～12:00，14:00～17:00。

Quidway(config)#settr 8:30 12:00 14:00 17:00

例：设置时间段为晚上 9:00 到早上 8:00。

Quidway(config)#settr 21:00 23:59 0:00 8:00

4）show access-list 命令

使用此命令来显示所指定的规则，同时查看规则过滤报文的情况。每个规则都有一个相应的计数器，如果用此规则过滤了一个报文，则计数器加 1；通过对计数器的观察可以看出所配置的规则中，哪些规则是比较有效的，而哪些基本无效。可以通过带 interface 关键字的 show access-list 命令来查看某个接口应用规则的情况。

该命令在特权用户配置模式下使用，命令格式为：

```
show access-list [ all | listnumber | interface interface-name ]
```

【参数说明】

all 表示所有的规则，包括普通时间段内及特殊时间段内的规则。

listnumber 为显示当前所使用的规则中序号为 listnumber 的规则。

interface 表示要显示在指定接口上应用的规则序号。

interface-name 为接口的名称。

例：显示当前所使用的序号为 100 的规则。

```
Quidway#show access-list 100
!
Using normal packet-filtering access rules now.
100 deny icmp 10.1.0.0 0.0.255.255 any host-redirect (3 matches,252 bytes
-- rule 1)
```

```
100 permit icmp 10.1.0.0 0.0.255.255 any echo (no matches -- rule 2)
100 deny udp any any eq rip (no matches -- rule 3)
!
```

例：显示接口 Serial0 上应用规则的情况。

```
Quidway#show access-list interface serial 0
!
Serial0:
access-list filtering In-bound packets : 120
access-list filtering Out-bound packets: None
!
```

5）show firewall 命令

使用此命令来显示防火墙的状态，包括防火墙是否被启用，启用防火墙时是否采用了时间段包过滤及防火墙的一些统计信息。

该命令在特权用户配置模式下使用，命令格式为：

```
show firewall
```

例：显示防火墙状态。

```
Quidway#show firewall
!
Firewall is enable, default filtering method is 'permit'.
TimeRange packet-filtering enable.
InBound packets: None;
OutBound packets: 0 packets, 0 bytes, 0% permitted,
0 packets, 0 bytes, 0% denied,
2 packets, 104 bytes, 100% permitted defaultly,
0 packets, 0 bytes, 100% denied defaultly.
From 00:13:02 to 06:13:21: 0 packets, 0 bytes, permitted.
!
```

6）管道命令（conduit）

前面讲过使用 static 命令可以在一个本地 IP 地址和一个全局 IP 地址之间创建了一个静态映射，但从外部到内部接口的连接仍然会被 pix 防火墙的自适应安全算法（ASA）阻挡，conduit 命令用来允许数据流从具有较低安全级别的接口流向具有较高安全级别的接口，例如允许从外部到 DMZ 或内部接口方向的会话。对于向内部接口的连接，static 和 conduit 命令将一起使用，来指定会话的建立。

conduit 命令配置语法：

```
conduit permit | deny global_ip port[-port] protocol foreign_ip [netm
ask]
```

【参数说明】

permit | deny： 允许 | 拒绝访问 。

global_ip 指的是先前由 global 或 static 命令定义的全局 IP 地址，如果 global_ip 为 0，就用 any 代替 0；如果 global_ip 是一台主机，就用 host 命令参数。

port 指的是服务所作用的端口，例如 www 使用 80，smtp 使用 25 等等，我们可以通过服务名称或端口数字来指定端口。

protocol 指的是连接协议，如 TCP，UDP，ICMP 等。

foreign_ip 表示可访问 global_ip 的外部 IP。对于任意主机，可以用 any 表示。如果 foreign_ip 是一台主机，就用 host 命令参数。

例：Pix525(config)#conduit permit tcp host 192.168.0.8 eq www any

这个例子表示允许任何外部主机对全局地址 192.168.0.8 的这台主机进行 http 访问。其中使用 eq 和一个端口来允许或拒绝对这个端口的访问。Eq ftp 就是指允许或拒绝只对 ftp 的访问。

例：Pix525(config)#conduit deny tcp any eq ftp host 61.144.51.89

表示不允许外部主机 61.144.51.89 对任何全局地址进行 ftp 访问。

例：Pix525(config)#conduit permit icmp any any

表示允许 icmp 消息向内部和外部通过。

例：Pix525(config)#static (inside, outside) 61.144.51.62 192.168.0.3

Pix525(config)#conduit permit tcp host 61.144.51.62 eq www any

这个例子说明 static 和 conduit 的关系。192.168.0.3 在内网是一台 Web 服务器，现在希望外网的用户能够通过 pix 防火墙得到 Web 服务。所以先做 static 静态映射：192.168.0.3→61.144.51.62（全局），然后利用 conduit 命令允许任何外部主机对全局地址 61.144.51.62 进行 http 访问。

7）配置 fixup 协议

fixup 命令作用是启用、禁止、改变一个服务或协议通过 pix 防火墙，由 fixup 命令指定的端口是 pix 防火墙要侦听的服务。见下面例子：

例： Pix525(config)#fixup protocol ftp 21

启用 ftp 协议，并指定 ftp 的端口号为 21。

例：Pix525(config)#fixup protocol http 80

Pix525(config)#fixup protocol http 1080

为 http 协议指定 80 和 1080 两个端口。

例： Pix525(config)#no fixup protocol smtp 80

禁用 smtp 协议。

8）设置 telnet

telnet 有一个版本的变化。在 Pix OS 5.0 之前，只能从内部网络上的主机通过 telnet 访问 pix。在其后续版本中，可以在所有的接口上启用 telnet 到 pix 的访问。当从外部接口要 telnet 到 pix 防火墙时，telnet 数据流需要用 ipsec 提供保护，也就是说用户必须配置 pix 来建立一条到另外一台 pix，路由器或 vpn 客户端的 ipsec 隧道。

telnet 配置语法：

```
telnet local_ip [netmask]
```

【参数说明】

local_ip 表示被授权通过 telnet 访问到 pix 的 IP 地址。如果不设此项，pix 的配置方式只能由 console 进行。

15.2 入侵检测技术

入侵检测是一种主动保护自己免受攻击的网络安全技术。作为防火墙的合理补充，入侵检测技术能够帮助系统对付网络攻击，扩展了系统管理员的安全能力（包括安全审计、监视、攻击识别和响应），提高了信息安全基础结构的完整性。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行检测。

15.2.1 入侵检测原理

入侵（Intrusion）的定义：任何试图危害资源的完整性、可信度和可获取性的动作。

入侵检测（Intrusion Detection）：按 Webster 辞典定义，即发现或确定入侵行为存在或出现的动作。也就是发现、跟踪并记录计算机系统或计算机网络中的非授权行为，或发现并调查系统中可能为试图入侵或病毒感染所带来的异常活动。入侵检测作为一门新兴的安全技术，以其对网络系统的实时监测和快速响应的特性，逐渐发展成为保障网络系统安全的关键技术。其基本原理如图 15-3 所示。

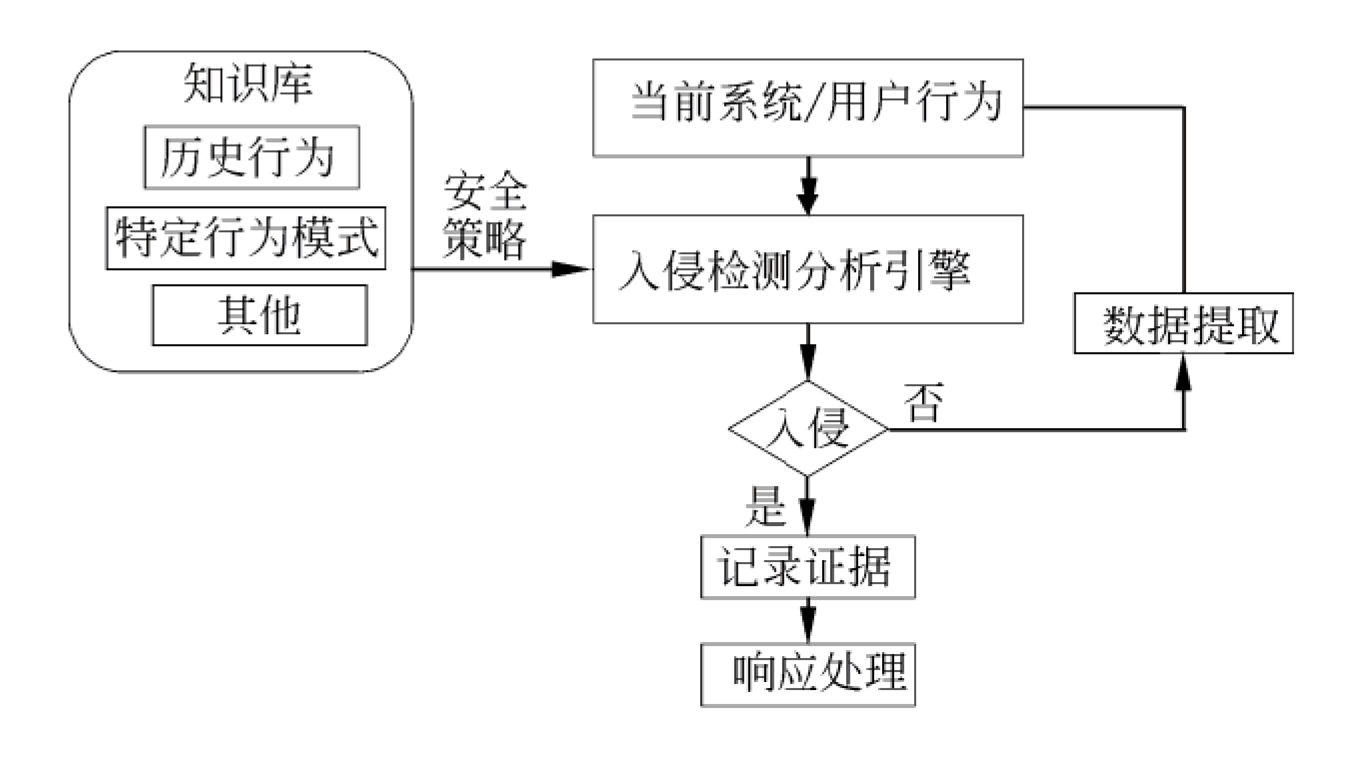


图 15-3 入侵检测原理

15.2.2　入侵检测系统的功能

入侵检测系统（Intrusion-detection system，IDS）是一种可应用于不同网络环境和不同系统的安全策略，IDS 在不同的应用环境中有不同的具体实现。从系统构成上看，入侵检测系统至少包括数据提取、入侵分析、响应处理三大部分，另外还可以结合安全知识库、数据存储等功能模块，提供更为完善的安全检测技术数据分析功能。

入侵检测系统模块结构如图 15-4 所示。

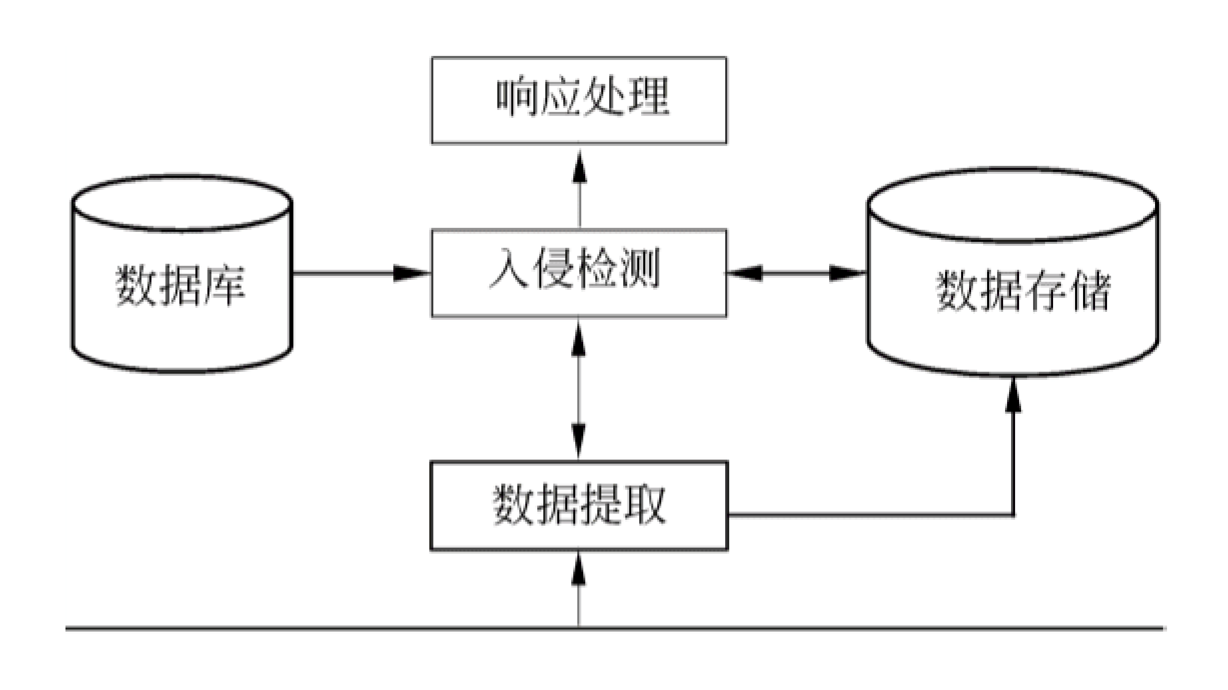


图 15-4　入侵检测系统模块结构

数据提取模块在入侵检测系统中居于基础地位，负责提取反映受保护系统运行状态的运行数据，并完成数据的过滤及其他预处理工作，为入侵分析模块和数据存储模块提供原始的安全审计数据，是入侵检测系统的数据采集器。

入侵分析模块是入侵检测系统的核心模块，包括对原始数据进行同步、整理、组织、分类、特征提取以及各种类型的细致分析，提取其中所包含的系统活动特征或模式，用于正常和异常行为的判断。这种行为的鉴别可以实时进行，也可以是事后的分析。

响应处理模块的工作实际上反映了当发现了入侵者的攻击行为之后，我们该怎么办的问题。可选的相应措施包括主动响应和被动响应。前者以自动的或用户设置的方式阻断攻击过程，后者则只对发生的时间进行报告和记录，由安全管理员负责下一步的行动。

IDS 具有以下的优点：

（1）实时检测网络系统的非法行为。

（2）网络 IDS 系统不占用系统的任何资源。

（3）网络 IDS 系统是一个独立的网络设备，可以做到对黑客不透明，因此其自身的安全性很高。

（4）网络 IDS 系统及时实时监测系统，也是记录审计系统，它可以做到实时保护和事后取证分析。

（5）主机 IDS 系统运行于保护系统之上，可以直接保护和恢复系统。

（6）通过与防火墙的连动，可以更有效地阻止非法入侵和破坏。

15.2.3 入侵检测系统的构成

IETF 将一个入侵检测系统分为四个组件：事件产生器（Event Generators）、事件分析器（Event Analyzers）、响应单元（Response Units）和事件数据库（Event Databases）。

（1）事件产生器的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。

（2）事件分析器分析得到的数据，并产生分析结果。

（3）响应单元则是对分析结果做出反应的功能单元，它可以作出切断连接、改变文件属性等强烈反应，也可以只是简单的报警。

（4）事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

15.2.4 入侵检测系统的分类

入侵检测系统一般有两种分类方法。一种是基于数据源的分类，另一种是基于检测方法的分类。

1．基于数据源的分类

入侵检测系统首先需要解决的问题是数据源，或者说是审计事件发生器。入侵检测系统根据其检测数据来源分为两类，分别是基于主机（Host-based）的入侵检测系统和基于网络（Network-based）的入侵检测系统。

（1）基于主机：安全操作系统必须具备一定的审计功能，并记录相应的安全性日志。

（2）基于网络：IDS 可以放在防火墙或者网关的后面，以网络嗅探器的形式捕获所有的对内对外的数据包。

两种入侵检测系统的比较如表 15-2 所示。

表 15-2 两种入侵检测系统的比较

系统类型	说明	优点
基于网络	使用原始的网络分组数据包作为进行攻击分析的数据源，一般利用一个网络适配器来实时监视和分析所有通过网络进行传输的通信。一旦检测到攻击，IDS 应答模块通过通知、报警以及中断连接等方式来对攻击做出反应	（1）成本低；（2）攻击者转移证据很困难；（3）实时检测和应答一旦发生恶意访问或攻击，基于网络的 IDS 检测可以随时发现它们，因此能够更快地做出反应。从而将入侵活动对系统的破坏减到最低；（4）能够检测未成功的攻击企图；（5）操作系统独立
基于主机	一般监视系统文件、事件、安全日志。一旦发现这些文件发生任何变化，IDS 将比较新的日志记录与攻击签名以发现它们是否匹配。如果匹配的话，检测系统就向管理员发出入侵报警并且发出采取相应的行动	（1）非常适用于加密和交换环境；（2）近实时的检测和应答；（3）不需要额外的硬件

基于网络的 IDS 并不依赖主机的操作系统作为检测资源。而基于主机的系统需要特定的操作系统才能发挥作用。

2．基于检测方法的分类

从检测方法上可以将入侵检测系统分为异常检测和误用检测两种类型。

（1）异常检测：也称为基于行为的检测。首先建立起用户的正常使用模式，即知识库，标识出不符合正常模式的行为活动。

（2）误用检测：也称为基于特征的检测。建立起已知攻击的知识库，判别当前行为活动是否符合已知的攻击模式。

15.2.5　入侵检测的主要方法

入侵检测的主要方法分为静态配置分析、异常性检测方法、基于行为的检测方法三种。

1．静态配置分析

静态配置分析通过检查系统的当前系统配置，诸如系统文件的内容或者系统表，来检查系统是否已经或者可能会遭到破坏。静态是指检查系统的静态特征（系统配置信息），而不是系统中的活动。

采用静态分析方法主要有以下几方面的原因：入侵者对系统攻击时可能会留下痕迹，这可通过检查系统的状态检测出来；系统管理员以及用户在建立系统时难免会出现一些错误或遗漏一些系统的安全性措施；另外系统在遭受攻击后，入侵者可能会在系统中安装一些安全性后门以方便对系统进行进一步的攻击。

所以静态配置分析方法需要尽可能了解系统的缺陷，否则入侵者只需要简单地利用那些系统中未知的安全缺陷就可以避开检测系统。

2．异常性检测方法

异常性检测技术是一种在不需要操作系统及其防范安全性缺陷专门知识的情况下，就可以检测入侵者的方法，同时它也是检测冒充合法用户的入侵者的有效方法。但是在许多环境中，为用户建立正常行为模式的特征轮廓及对用户活动的异常性进行报警的门限值的确定都是比较困难的事，所以仅使用异常性检测技术不可能检测出所有的入侵行为。

目前这类入侵检测系统多采用统计，或者基于规则描述的方法来建立系统主体的行为特征轮廓：

（1）统计性特征轮廓由主体特征变量的频度、均值以及偏差等统计量来描述，如 SRI 的下一代实时入侵检测专家系统，这种方法对特洛伊木马以及欺骗性的应用程序的检测非常有效。

（2）基于规则描述的特征轮廓，由一组用于描述主体每个特征的合法取值范围与其

他特征的取值之间关系的规则组成（如 TIM）。该方案还可以采用从大型数据库中提取规则的数据挖掘技术。

（3）神经网络方法具有自学习、自适应能力，可以通过自学习提取正常的用户或系统活动的特征模式，避开选择统计特征这一难题。

3．基于行为的检测方法

通过检测用户行为中那些与已知入侵行为模式类似的行为，那些利用系统中缺陷或间接违背系统安全规则的行为，来判断系统中的入侵活动。

目前基于行为的入侵检测系统只是在表示入侵模式（签名）的方式以及在系统的审计中检查入侵签名的机制上有所区别，主要可以分为基于专家系统、基于状态迁移分析和基于模式匹配等几类。这些方法的主要局限在于，只是根据已知的入侵序列和系统缺陷模式来检测系统中的可疑行为，而不能检测新的入侵攻击行为以及未知的、潜在的系统缺陷。

入侵检测方法虽然能够在某些方面取得好的效果，但总体看来各有不足，因而越来越多的入侵检测系统都同时采用几种方法，以互补不足，共同完成检测任务。

15.3 加密与密钥管理技术

希赛教育专家特别提示：本节考点主要涉及加密技术与密钥管理技术的相关内容，在历年考试中均屡次涉及。

15.3.1 加密体制

加密就是指对数据进行编码变换使其看起来毫无意义，但同时却仍可以保持其可恢复的形式的过程。在这个过程中被变换的数据称为明文，它可以是一段有意义的文字或者数据，变换过后的形式称为密文，看起来毫无意义。加密机制有助于保护信息的机密性和完整性，有助于识别信息的来源，它可能是最广泛使用的安全机制。

加密算法分为私钥加密算法和公钥加密算法。其中私钥加密算法又称为对称加密算法，公钥加密算法又称为不对称加密算法。

本知识点主要是掌握对称密钥技术和非对称密钥技术的区别与主要特点，了解对称密钥技术的代表 DES、3DES、IDEA 以及非对称密钥技术的代表 RSA 的主要技术特征，特别要注意 RSA 算法。

1．对称密钥技术

对称密钥技术是指加密系统的加密密钥和解密密钥相同，或者虽然不同，但从其中的任意一个可以很容易地推导出另一个。其优点是具有很高的保密强度，但密钥的传输需要经过安全可靠的途径。

对称密码技术有两种基本类型：分组密码（它是在明文分组和密文分组上进行运算）和序列密码（对明文和密文数据流按位或字节进行运算）。常见的对称密钥技术包括：

（1）DES：它是一种迭代的分组密码，输入输出都是 64 位，使用一个 56 位的密钥以及附加的 8 位奇偶校验位，有弱钥，但可避免。攻击 DES 的主要技术是穷举。但由于 DES 的密钥长度较短，因此为了提高安全性，就出现了使用 112 位密钥对数据进行三次加密的算法，称为 3DES。

（2）IDEA 算法：其明文和密文都是 64 位，密钥长度为 128 位。

2．非对称密钥技术

非对称密钥技术也称为公钥算法，就是指加密系统的加密密钥和解密密钥完全不同，并且不可能从任何一个推导出另一个。它的优点在于可以适应开放性的使用环境，可以实现数字签名与验证。

最常见的非对称密钥技术就是 RSA。理论基础是数论中大素数分解，但如果使用 RSA 来加密大量的数据则速度太慢，效率不高，因此 RSA 广泛用于密钥的分发（对会话密钥进行加密）。公开密钥算法现在主要的两大类算法是：建立在基于“分解大数的困难度”基础上的算法和建立在“以大素数为模来计算离散对数的困难度”基础上的算法，至今数学家研究多年，还没有能够完全破解。

15.3.2　密钥管理技术

密钥是加密算法中的可变部分，在采用加密技术保护的信息系统中，其安全性取决于密钥的保护，而不是对算法或硬件保护。密码机制可以公开，密码设备可能丢失，但同一型号的密码机仍可继续使用。然而密钥一旦丢失或出错，不但合法用户不能提取信息，而且可能是非法用户窃取信息。因此，密钥的管理是关键问题。

密钥管理是指处理密钥自产生到销毁的整个过程中的有关问题，包括系统的初始化、密钥的产生、存储、备份/恢复、装入、分配、保护、更新、控制、丢失、吊销及销毁。当前主要的密钥管理体制有三种：适用于封闭网，以传统的密钥管理中心为代表的 KMI 机制；适用于开放网的 PKI 机制；适用于规模化专用网的 SPK 机制。

1．KMI 机制

密钥管理基础结构 KMI 设定一个密钥分配中心 KDC 来负责发放密钥。这种结构经历了从静态发放到动态发放的发展过程，目前仍然是密钥管理的重要手段。无论是静态发放或是动态发放，都依赖于秘密信道，其特点如表 15-3 所示。

表 15-3　密钥分发机制

分 发 类 型	技　　术	特　　点
静态分发	点对点配置	可用单钥或双钥实现。单钥为鉴别提供可靠参数，但不提供不可否认服务。数字签名要求双钥实现

续表

分发类型	技术	特点
静态分发	一对多配置	可用单钥或双钥实现。只在中心保留所有各端的密钥，各端只保留自己的密钥。是建立秘密通道的主要办法
	格状网配置	可用单钥或双钥实现。也称为端端密钥，密钥配置量为全网 n 个终端中选 2 的组合数
动态分发	基于单钥的单钥分发	首先用静态分发方式配置的星状密钥配置，主要解决会话密钥的分发
	基于单钥的双钥分发	公私钥对都当做秘密变量

2．PKI 机制

PKI（Public Key Infrustructure）又称为公钥基础设施，是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。PKI 机制解决了分发密钥时依赖秘密信道的问题。

完整的 PKI 系统必须具有权威认证机关（CA）、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口等基本构成部分，构建 PKI 也将围绕着这五大系统来着手构建。PKI 机制与 KMI 机制比较如表 15-4 所示。

表 15-4　PKI 与 KMI 比较

项目	PKI	KMI
作用特性	良好的扩展性，适于开放业务	很好的封闭性，适于专用业务
服务功能	只提供数字签名服务	提供加密和签名功能
信任逻辑	第三方管理模式	集中式的主管方管理模式
负责性	个人负责的技术体系	单位负责制
应用角度	主外	主内

3．SPK 机制

为了更好地解决密钥管理的问题，现在提出了种子化公钥（SPK）和种子化双钥（SDK）体系。在 SPK 体制中可以实现：

（1）多重公钥（双钥），即 LPK/LDK，用 RSA 公钥算法实现。

（2）组合公钥（双钥），即 CPK/CDK，用离散对数 DLP 或椭圆曲线密码 ECC 实现。它是电子商务和电子政务中比较理想的密钥解决方案。

15.4　数字签名与数字证书

本知识点在于了解数字签名技术的概念与应用，理解其工作的原理，以及数字证书的体系、内容、格式、证书获取及吊销等关键性概念。

1．数字签名

简单地说，所谓数字签名就是附加在数据单元上的一些数据，或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人（例如接收者）进行伪造。它是对电子形式的消息进行签名的一种方法，一个签名消息能在一个通信网络中传输。基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名。包括普通数字签名和特殊数字签名。普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Des/DSA，椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等，它与具体应用环境密切相关。显然，数字签名的应用涉及到法律问题，美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准（DSS）。

数字签名必须保证以下三点：

（1）接收者能够核实发送者对报文的签名。

（2）发送者事后不能抵赖对报文的签名。

（3）接收者不能伪造对报文的签名。

数字签名主要的功能是：保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

Hash 签名是最主要的数字签名方法，也称之为数字摘要法（Digital Digest）或数字指纹法（Digital Finger Print）。它与 RSA 数字签名是不同的，该数字签名方法是将数字签名与要发送的信息紧密联系在一起，它更适合于电子商务活动。将一个商务合同的个体内容与签名结合在一起，并将合同和签名分开传递，更增加了可信度和安全性。

数字摘要加密方法亦称安全 Hash 编码法（SHA）或 MD5。该编码法采用单向 Hash 函数将需加密的明文“摘要”成一串 128bit 的密文，这一串密文亦称为数字指纹（Finger Print），它有固定的长度，且不同的明文摘要必定一致。这样这串摘要就可成为验证明文是否是“真身”的“指纹”了。

2．数字证书

数字证书又称为数字标识（Digital Certificate，Digital ID），是由证书签证机关（CA）签发的对用户的公钥的认证。因此，证书的内容应包括 CA 的信息、用户信息、用户公钥及 CA 签发时间及有效期等内容。目前国际上对证书的格式及认证方法遵从 X.509 体系标准。

数字证书实际上是一份电子文档，是一段包含用户身份信息、用户公钥信息以及身份验证机构数字签名的数据。身份验证机构的数字签名可以确保证书信息的真实性。证书格式及证书内容遵循 X.509 标准。

1）数字证书的格式

数字证书的格式一般使用 X.509 国际标准。X.509 是广泛使用的证书格式之一，X.509

用户公钥证书是由可信赖的证书权威机构（CA——证书授权中心）创建的，并且由 CA 将用户存放在 X.500 的目录中。

在 X.509 格式中，数字证书通常包括：版本号、序列号（CA 下发的每个证书的序列号都是唯一的）、签名算法标识符、发行者名称、有效性、主体名称、主体的公开密钥信息、发行者唯一识别符、主体唯一识别符、扩充域、签名（就是 CA 用自己的私钥对上述域进行数字签名的结果，也可以理解为是 CA 中心对用户证书的签名）等。

2）数字证书的获取

任何一个用户只要得到 CA 中心的公钥，就可以得到该 CA 中心为该用户签署的数字证书。因为证书是不可伪造的，因此对于存放证书的目录无须施加特别的保护。

因为用户数量多，因此会存在多个 CA 中心。但如果两个用户使用的是不同 CA 中心发放的证书，则无法直接使用证书；但如果两个证书发放机构之间已经安全地交换了公开密钥，则可以使用证书链来完成通信。

3）数字证书的吊销

证书到了有效期、用户私钥已泄露、用户放弃使用原 CA 中心的服务、CA 中心私钥泄露都需吊销证书，这时 CA 中心会维护一个证书吊销列表 CRL，供大家查询。

15.5 虚拟专用网

虚拟专用网（Virtual Private Network，VPN）是企业网在因特网等公共网络上的延伸，通过一个私有的通道在公共网络上创建一个安全的私有连接。因此，从本质上说 VPN 是一个虚信道，它可用来连接两个专用网，通过可靠的加密技术方法保证其安全性，并且是作为一个公共网络的一部分存在的。

图 15-5 就是一个 VPN 构成的原理示意图。

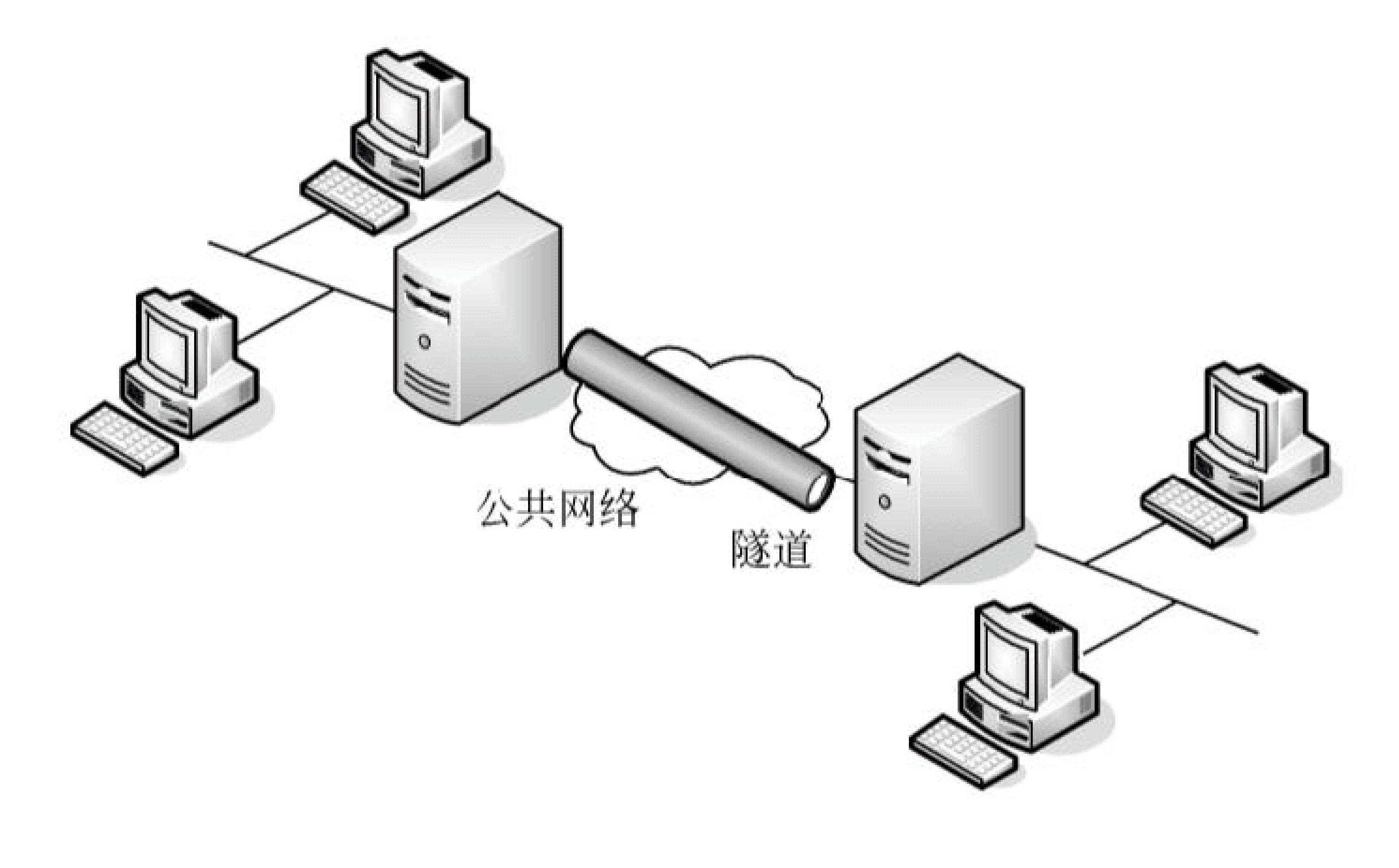


图 15-5 VPN 原理示意图

1．VPN 的关键技术

目前 VPN 主要采用四项技术来保证安全，这四项技术分别是隧道技术、加解密技术、密钥管理技术、使用者与设备身份认证技术。

（1）隧道技术是 VPN 的基本技术，类似于点对点连接技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。

第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有 L2F、PPTP、L2TP 等。

第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有 VTP、IPSec 等。

（2）加解密技术是数据通信中一项较成熟的技术，VPN 可直接利用现有技术。

（3）密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。

（4）身份认证技术最常用的是使用者名称与密码或卡片式认证等方式。

2．PPP 回话过程

PPP 拨号会话过程可以分成四个不同的阶段，分别是：创建 PPP 链路、用户验证、PPP 回叫控制、调用网络层协议。在第二阶段，客户 PC 会将用户的身份名发给远端的接入服务器。该阶段使用一种安全认证方式避免第三方窃取数据或冒充远程客户接管与客户端的连接。大多数的 PPP 方案只提供了有限的认证方式，包括口令字认证协议（PAP），挑战握手认证协议（CHAP）和微软挑战握手认证协议（MS-CHAP）。

（1）口令字认证协议（PAP）。PAP 是一种简单的明文认证方式。NAS 要求用户提供用户名和口令，PAP 以明文方式返回用户信息。很明显，这种认证方式的安全性较差，第三方可以很容易地获取被传送的用户名和口令，并利用这些信息与 NAS 建立连接，获取 NAS 提供的所有资源。所以，一旦用户密码被第三方窃取，PAP 无法提供避免受到第三方攻击的保障措施。

（2）挑战握手认证协议（CHAP）。CHAP 是一种加密的认证方式，能够避免建立连接时传送用户的真实密码。NAS 向远程用户发送一个挑战口令（challenge），其中包括会话 ID 和一个任意生成的挑战字串。远程客户必须使用 MD5 单向哈希算法返回用户名和加密的挑战口令、会话 ID 以及用户口令，其中用户名以非哈希方式发送。CHAP 为每一次认证任意生成一个挑战字串来防止受到再现攻击。在整个连接过程中，CHAP 将不定时地向客户端重复发送挑战口令，从而避免第三方冒充远程客户进行攻击。

15.6　电子商务安全

本知识点主要在于掌握电子商务安全的基本需求、安全协议以及相关的技术。

1．电子商务安全特性

电子商务是指利用简单、快捷、低成本的电子通信方式，买卖双方不谋面地进行各种商贸活动。对于电子商务安全需求主要表现在：

（1）有效性：即要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，以保证贸易数据在确定的时刻、地点是有效的。

（2）机密性：要预防非法的信息存取和信息在传输过程中被非法窃取。

（3）数据完整性：要求能够保证数据的一致性，防止数据被非授权者建立、修改和破坏。

（4）不可抵赖性：也就是防止交易的某方否认曾经发生的交易行为。

（5）审查能力：根据机密性和完整性的要求，应对数据审查的结果进行记录。

与电子商务相关的安全技术主要包括：VPN、SSL、电子邮件安全协议（包括 PEM、S/MIME、MOSS）、电子支付安全性等。

2．SSL/SET 和 SHTTP

SSL，安全套接层，是工作在传输层的安全协议。它结合了信息加解密、数字签名与签证两大技术。它包括协商层（SSL Handshake）和记录层（SSL Record）两个部分。

（1）协商层：包括“沟通”通信中所使用的 SSL 版本、信息加密用的算法、所使用的公钥算法，并要求用公钥方式对客户端进行身份认证。

（2）记录层：对应用程序提供的信息进行分段、压缩、数据认证与加密，能够保障数据的机密性和报文的完整性。整个操作步骤如下：

第一步：分片，分成 214 字节或更小的数据块；

第二步：可选地应用压缩；

第三步：使用共享的密钥计算出报文鉴别代码；

第四步：使用同步算法加密；

第五步：附加首部，包括内容类型、主要版本、次要版本、压缩长度。

SHTTP 是在 HTTP 协议上的扩展，目的是保证商业贸易的传输安全，工作于应用层。由于 SSL 的迅速出现，加上 SSL 工作在传输层，适用于所有 TCP/IP 应用，而 SHTTP 只能够工作于 HTTP 协议层，只限于 Web 应用，因此 SHTTP 并未能够获得广泛应用。

SET 协议是 Visa 与 MasterCard 共同制定的一套安全又方便的交易模式，最早用于支持各种信用卡的交易。SSL 在使用时，只要求服务器端拥有数字证书，而 SET 则同时要求客户端需要数字证书。SET 可以实现：在交易涉及的各方间提供安全的通信信道，通过使用 X.509 数字证书来提供信任，可以保证信息的机密性。

SET 协议的参与者有：卡用户（网上交易发起方）、商人（网上交易服务商）、发行人——银行（信用卡发卡人）、获得者（处理交易的金融机构）、支付网关、CA 中心（发放证书者）。

3．PGP 技术

目前，PGP 协议在互联网上被广泛采用，特别在 E-mail 保护上应用更广，它是结合了 RSA 和 IDEA 的链式加密法。PGP 的工作过程是用一个随机生成的密钥（每次加密不同）用 IDEA 算法对明文加密，然后用 RSA 算法对该密钥加密。因此它既有了 RSA 的保密性，又获得了 IDEA 算法的快捷性。

4．Kerberos

在分布式网络应用环境中，要保证其使用的安全性，就必须让工作站能够用可信、安全的方式向服务器证实其身份，否则就会出现许多安全问题。而解决这个问题的技术称之为身份认证。比较常见的身份认证技术包括：用户双方指定共享密钥（最不安全）、使用智能卡生成密钥、使用 Kerberos 服务、使用 PKI 服务（即通过从 CA 中心获取数字证书的方式）。

Kerberos 并非为每一个服务器构造一个身份认证协议，而是提供一个中心认证服务器，提供用户到服务器以及服务器到用户的认证服务。Kerberos 的核心是使用 DES 加密技术，实现最基本的认证服务。

如图 15-6 所示，Kerberos 认证过程可以分为三个阶段，六个步骤。

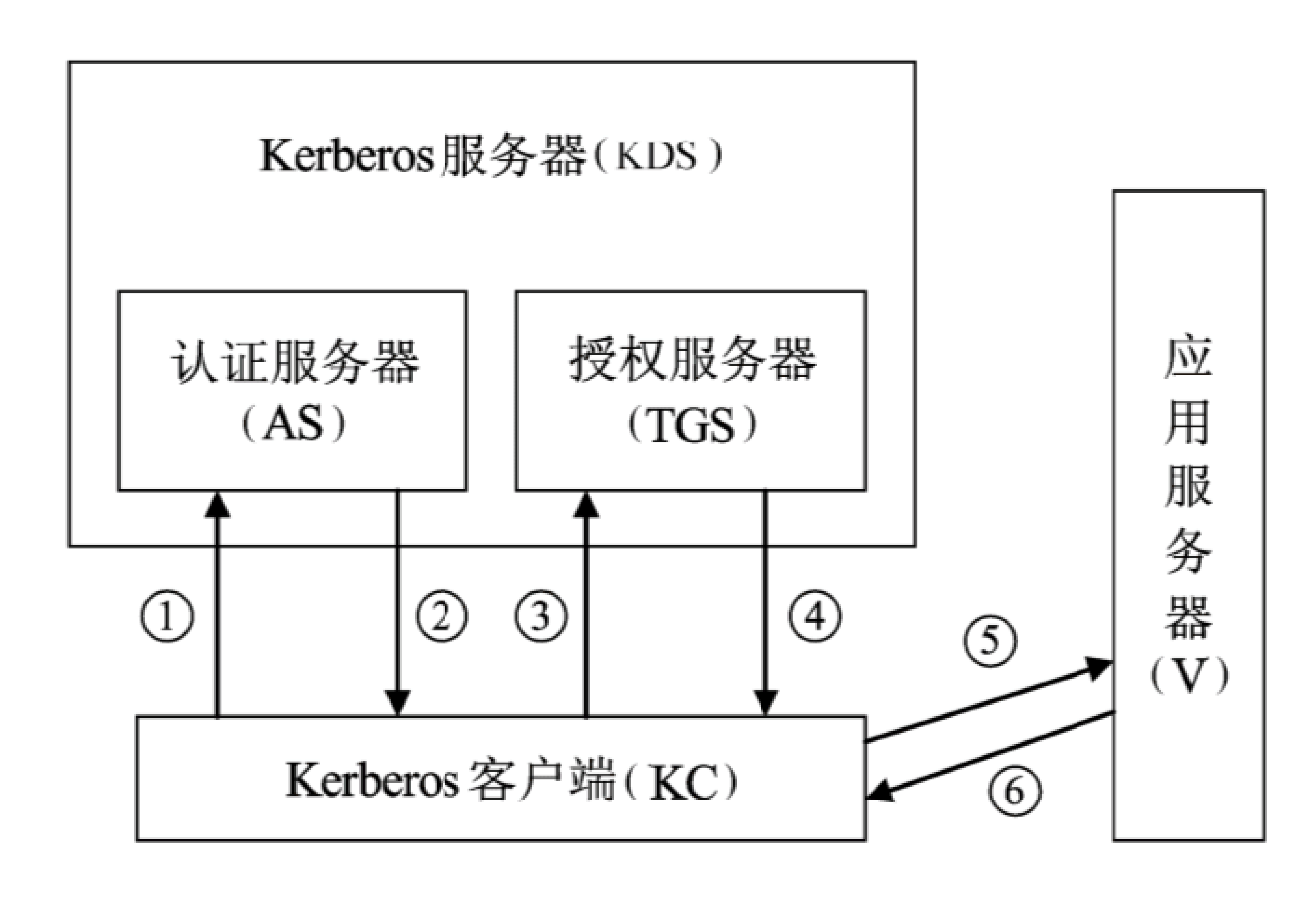


图 15-6　Kerberos 工作原理示意图

第一阶段：认证服务交换、客户端获取授权服务器访问许可票据。

① 用户 A 输入自己的用户名，以明文的方式发给认证服务器。

② 认证服务器返回一个会话密钥 K_S 和一个票据 K_{TGS}（A,K_S），这个会话密钥是一次性的（也可以使用智能卡生成），而这两个数据包则是使用用户 A 的密钥加密的，返回时将要求其输入密码，并解密数据。

第二阶段：票据许可服务交换，客户端获得应用服务访问许可票据。

③ 用户 A 将获得的票据、要访问的应用服务器名 B，以及用会话密钥加密的时间标记（用来防止重发攻击）发送给授权服务器（TGS）。

④ 授权服务器（TGS）收到后，返回 A 和 B 通信的会话密钥，包括用 A 的密钥加密的，和 B 的密钥加密的会话密钥 K_{AB}。

第三阶段：客户端与应用服务器认证交换，客户端最终获得应用服务。

⑤ 用户 A 将从 TGS 收到的用 B 的密钥加密的会话密钥发给服务器 B，并且附上用双方的会话密钥 K_{AB} 加密的时间标记以防止重发攻击。

⑥ 服务器 B 进行应答，完成认证过程。

从上面的描述中可以看出，Kerberos 采用了连续加密的机制来防止会话被劫持。

15.7 例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 8 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

按实现原理的不同将防火墙分为__（1）__三类。

（1）A．包过滤防火墙、应用层网关防火墙和状态检测防火墙

B．包过滤防火墙、应用层网关防火墙和代理防火墙

C．包过滤防火墙、代理防火墙和软件防火墙

D．状态检测防火墙、代理防火墙和动态包过滤防火墙

例题 1 分析

防火墙主要有三种类型：包过滤防火墙、应用网关防火墙和状态检测防火墙。

包过滤防火墙工作在网络层，它可以对 TCP/IP 数据包的源地址、目的地址、源端口和目的端口进行过滤。它的优点是效率比较高，对用户来说是透明的，用户可能不会感觉到包过滤防火墙的存在，除非他是非法用户被拒绝了。缺点是对于大多数服务和协议不能提供安全保障，无法有效地区分同一 IP 地址的不同用户，并且包过滤防火墙难于配置、监控和管理，不能提供足够的日志和报警。

应用网关防火墙在应用层实现防火墙的功能，它使用一个客户程序与特定的中间节点（防火墙）连接，然后中间节点与服务器进行实际连接。与包过滤防火墙所不同的是，使用这种类型的防火墙，外部网络之间不存在直接连接，因此即使防火墙发生了问题，外部网络也无法获得与被保护的网络的连接。应用网关防火墙提供了详细的日志及审计功能，大大提高了网络的安全性，也为改进现有软件的安全性能提供了可能。应用网关防火墙是基于特定应用程序解决安全问题，基于 Proxy 的产品将被改进成能设置常用服务和非标准端口。然而只要应用程序需要升级，基于 Proxy 的用户会发现他们必须购买新的 Proxy server。一个明显的例子是许多 Web 浏览器中加入了大量的安全措施，防火墙的购买者应留心询问防火墙厂商他们的产品到底能处理哪些应用程序。作为一种网络安全技术，Firewall 结合 Proxy Server 具有简单实用的特点，可以在不修改原有网络应

用系统的情况下达到一定的安全要求。但是如果防火墙系统被攻破，则被保护的网络处于无保护状态。并且如果一个企业希望在 Internet 上开展商业活动，与众多的客户进行通信，则不能满足要求。另外基于 Proxy Service 的防火墙常常会使网络性能明显下降。根据报道，相当多的防火墙不能处理高负载的网络通信。在被测试的商业防火墙中，在 E1 条件下，没有一种不发生 session 丢失的情况。由于一种被称为“denial of service”的黑客手法对防火墙的网络性能提出了很高的要求，如果防火墙的网络性能太差，就很容易受到它的攻击。

以状态检测技术为核心的第三代防火墙，综合包过滤防火墙和应用网关防火墙于一身。状态检测防火墙通过状态检测模块，访问和分析从通信层得到的数据，实现防火墙的功能。它提供虚拟会话信息，可以支持 RPC（Remote Procedure Call 远程过程调用）和基于 UDP 协议的应用。并且这些“状态”和“上下文”可以动态地存储和升级。

无论何种类型防火墙，从总体上看，都应具有以下五大基本功能：

（1）过滤进、出网络的数据。

（2）管理进、出网络的访问行为。

（3）封堵某些禁止的业务。

（4）记录通过防火墙的信息内容和活动。

（5）对网络攻击的检测和告警。

例题 1 答案

（1）A

例题 2

网络通信中广泛使用的 DES 加密算法属于__（2）__。

（2）A. 对称加密　　B. 非对称加密

C. 公开密钥加密　　D. 不可逆加密

例题 2 分析

DES 算法为密码体制中的对称密码体制，又被称为美国数据加密标准，是 1972 年美国 IBM 公司研制的对称密码体制加密算法。其密钥长度为 56 位，明文按 64 位进行分组，将分组后的明文组和 56 位的密钥按位替代或交换的方法形成密文组的加密方法。

例题 2 答案

（2）A

例题 3

下面关于数字签名的说法中，不正确的是__（3）__。

（3）A. 数字签名可以保证数据的完整性

B. 发送方无法否认自己签发的消息

C. 接收方可以得到发送方的私钥

D. 接收方可以确认发送方的身份

例题 3 分析

数字签名使用公钥算法，整个数字签名应用过程很简单：

（1）信息发送者使用一单向散列函数对信息生成信息摘要。

（2）信息发送者使用自己的私钥签名信息摘要。

（3）信息发送者把信息本身和已签名的信息摘要一起发送出去。

（4）信息接收者通过使用与信息发送者使用的同一个单向散列函数对接收的信息本身生成新的信息摘要，再使用信息发送者的公钥对信息摘要进行验证，以确认信息发送者的身份是否被修改过。

（5）接受者只需使用发送者的公钥对信息摘要进行解密。

整个过程中，接收方不需要使用发送方的私钥。因此 C 不正确。

例题 3 答案

（3）C

例题 4

入侵检测系统无法__（4）__。

（4）A. 监测并分析用户和系统的活动

B. 评估系统关键资源数据文件的完整性

C. 识别已知的攻击行为

D. 发现 SSL 数据包中封装的病毒

例题 4 分析

入侵检测系统是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处在于，IDS 是一种积极主动的安全防护技术。它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

具体来说，入侵检测系统的主要功能有：

（1）监视、分析用户及系统活动。

（2）系统构造和弱点的审计。

（3）识别反映已知进攻的活动模式并向相关人士报警。

（4）异常行为模式的统计分析。

（5）评估重要系统和数据文件的完整性。

（6）操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

而对于封装在数据包中的病毒，入侵检测系统是无法检测的。

例题 4 答案

（4）D

例题 5

甲和乙采用公钥密码体制对数据文件进行加密传送，甲用乙的公钥加密数据文件，

乙使用__(5)__来对数据文件进行解密。

(5) A．甲的公钥　　B．甲的私钥　　C．乙的公钥　　D．乙的私钥

例题 5 分析

公钥加密和数字签名的应用流程如图 15-7 所示。

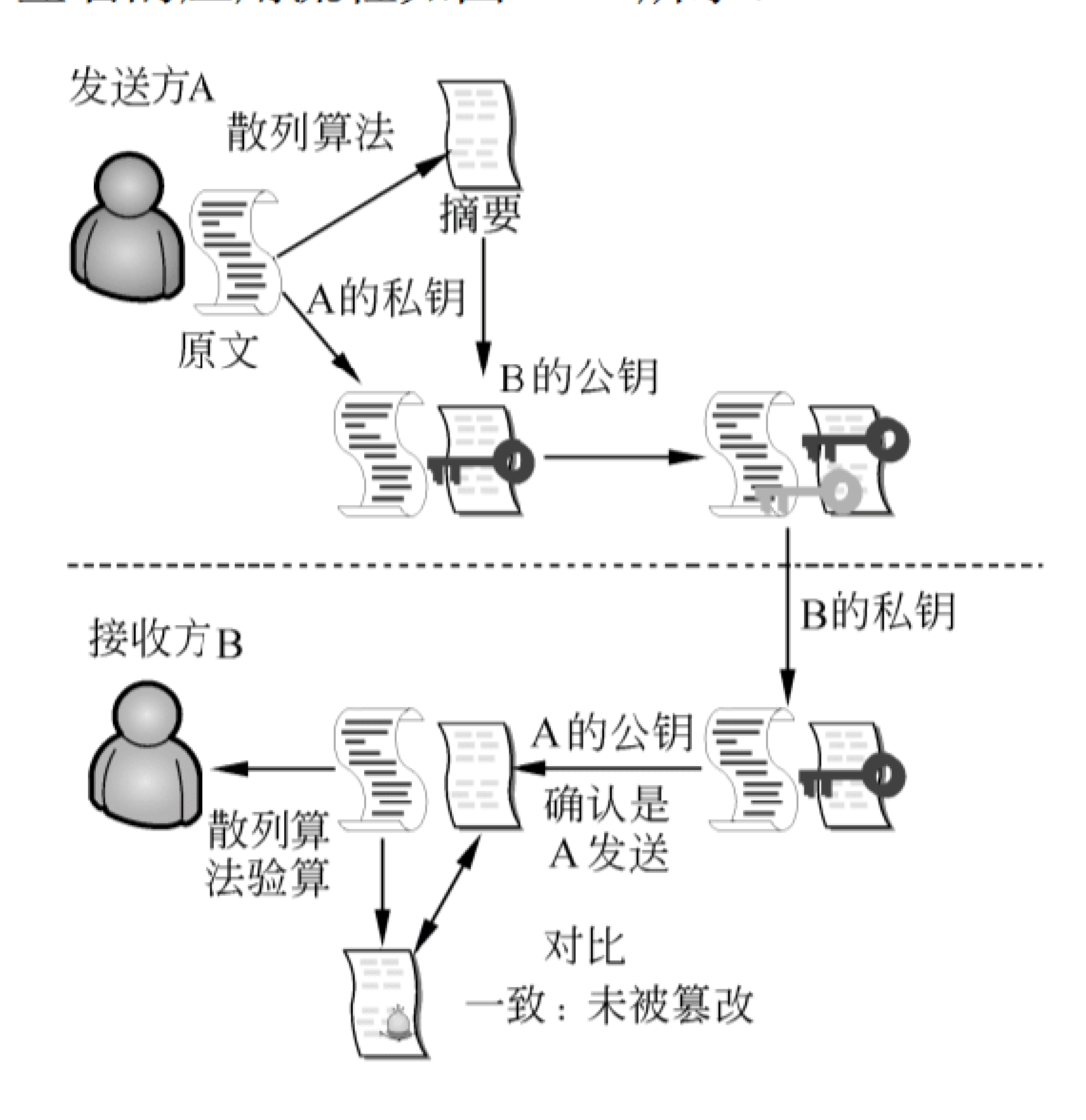


图 15-7　实际应用中的公钥加密和数字签名流程

发送方 A 先通过散列函数对要发送的信息（M）计算消息摘要（MD），也就是提取原文的特征。

发送方 A 将原文（M）和消息摘要（MD）用自己的私钥（PrA）进行加密，实际上就是完成签名动作，其信息可以表示为 PrA（M+MD）。

然后以接收方 B 的公钥（PB）作为会话密钥，对这个信息包进行再次加密，得到 PB（PrA（M+MD））。

当接收方收到消息后，首先用自己的私钥 PrB 进行解密，从而得到 PrA（M+MD）。

再利用 A 的公钥（PA）进行解密，如果能够解密，显然说明该数据是 A 发送的，同时也就将得到原文 M 和消息摘要 MD。

然后对原文 M 计算消息摘要，得到新的 MD，与收到的 MD 进行比较，显然如果一致说明该数据在传输时未被篡改。

至此，整个通信过程也就完成了。不过要注意的是，在实际的应用中，通常不会用 A 的私钥对原文进行加密，一方面是效率太低，另一方面是没有太大的必要。

例题 5 答案

(5) D

例题 6

在公司内网中部署__(6)__可以最大限度防范内部攻击。

（6）A. 防火墙　　B. 电磁泄密及防护系统

C. 邮件过滤系统　　D. 入侵检测系统

例题 6 分析

网络入侵检测系统位于有敏感数据需要保护的网络上，通过实时侦听网络数据流，寻找网络违规模式和未授权的网络访问尝试。在内部应用网络中的重要网段，使用网络探测引擎，监视并记录该网段上的所有操作，在一定程度上防止非法操作和恶意攻击网络中的重要服务器和主机。同时，网络监视器还可以形象地重现操作的过程，可帮助安全管理员发现网络安全的隐患。

例题 6 答案

（6）D

例题 7

某公司在 Windows 2003 中安装 IIS6.0 作为 Web 服务器，IP 地址为 211.120.114.3，端口号为 8080，并在 IIS 中配置 HTTPS 实现安全的 Web 通信，如图 15-8 所示。

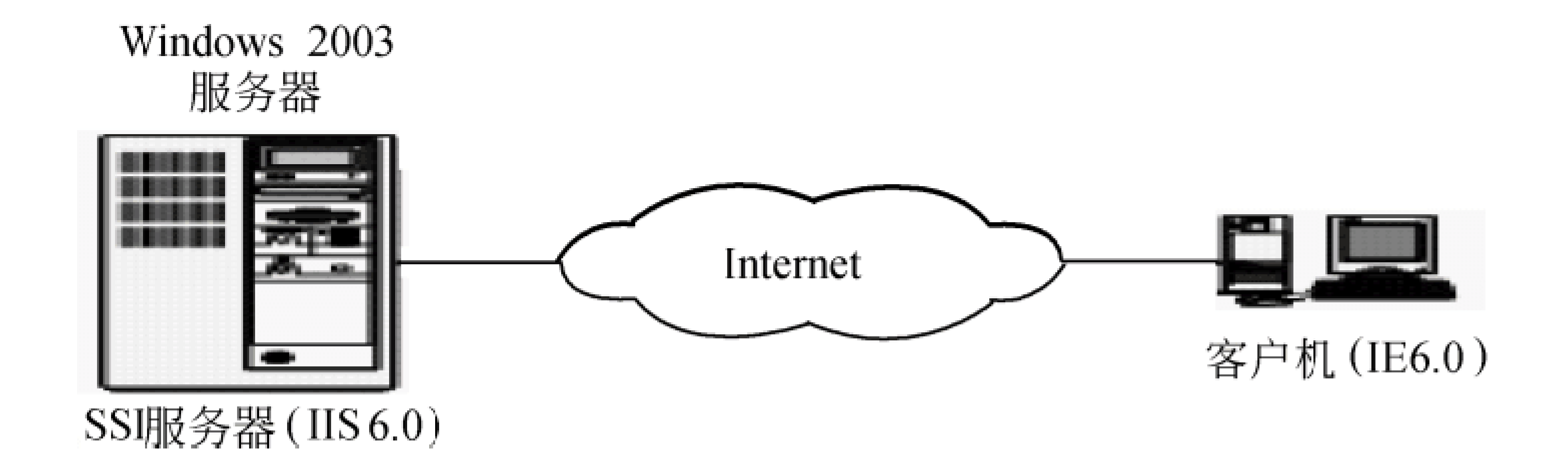


图 15-8　Web 通信

【问题 1】

IIS 6.0 安装的硬盘分区最好选用 NTFS 格式，是因为__（1）__和__（2）__。

（1）、（2）备选答案：

A. 可以防止网页中的 Applet 程序访问硬盘中的文件

B. 可以针对某个文件或文件夹给不同的用户分配不同的权限

C. 可以使用系统自带的文件加密系统对文件或文件夹进行加密

D. 可以在硬盘分区中建立虚拟目录

【问题 2】

HTTPS 工作在__（3）__层，为浏览器和 Web 服务器的提供安全信息交换，它运行在安全__（4）__之上。

（3）A. 网络层　　B. 传输层　　C. 应用层　　D. 会话层

（4）A. 网关　　B. 套接口　　C. 密钥　　D. 物理连接

【问题 3】

在配置 IIS 6.0 时，需首先向__（5）__申请并安装数字证书，然后 Web 服务器才能支持 SSL 会话。

在 IIS 中安装 SSL 分 5 个步骤，__（6）__→提交数字证书申请→__（7）__→在 IIS 服务器上导入并安装证书→__（8）__。

（6）～（8）备选答案：

A. 下载证书文件

B. 生成证书请求文件

C. 配置身份验证方式和 SSL 安全通道

【问题 4】

如果希望 Web 服务器只接收 HTTPS 请求，而不接受未加密的 HTTP 请求，加密密钥为 128 位，并且无需为客户端提供数字证书，在图 15-9 中该如何配置？

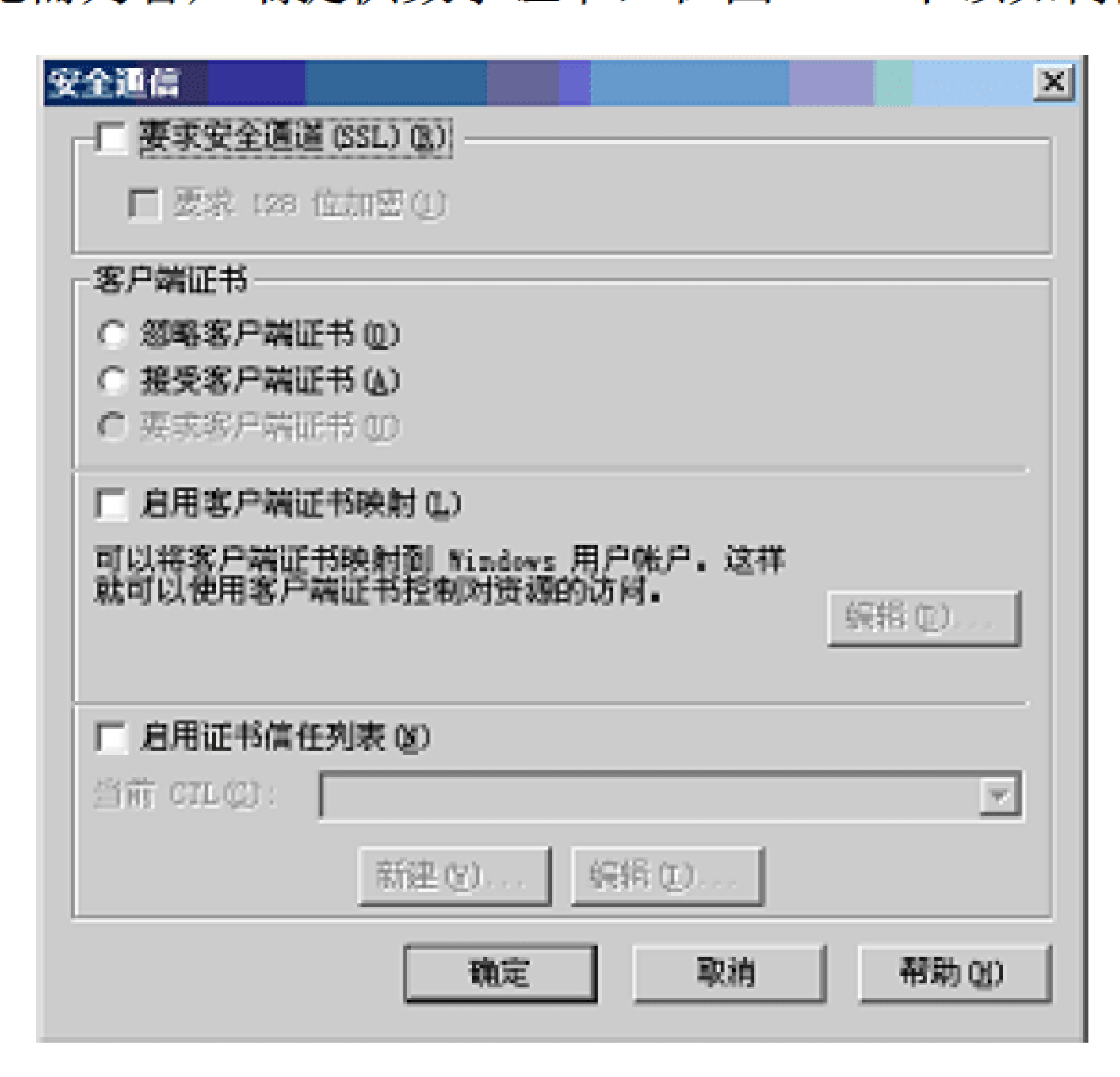


图 15-9　安全通信配置

【问题 5】

如果用户需要通过 SSL 安全通道访问该 Web 网站，可在 IE 的地址栏中输入__（9）__。

例题 7 分析

【问题 1】

本题考查 NTFS 格式文件系统管理的一些优势。NTFS 是 Windows NT 操作环境和 Windows NT 高级服务器网络操作系统环境的文件系统。在 NTFS 分区上，可以共享资源、文件夹及为文件设置访问许可权限。许可的设置包括两方面的内容：一是允许哪些组或用户对文件夹、文件和共享资源进行访问；二是获得访问许可的组或用户可以进行什么级别的访问。同时还可以使用系统自带的文件加密系统对文件或文件夹进行加密，

保证数据的安全可靠。

【问题 2】

本题考查 HTTPS 协议的相关知识。安全超文本传输协议（Secure Hypertext Transfer Protocol，HTTPS）是用于对数据进行压缩和解压操作，并返回网络上传送回的结果。HTTPS 实际上应用了 Netscape 的完全套接字层（SSL）作为 HTTP 应用层的子层。（HTTPS 使用端口 443，而不是像 HTTP 那样使用端口 80 来和 TCP/IP 进行通信）。SSL 使用 40 位关键字作为 RC4 流加密算法，这对于商业信息的加密是合适的。

HTTPS 工作在应用层，为浏览器和 Web 服务器提供安全信息交换，它运行在安全传输层之上。

【问题 3】

在配置 IIS6.0 时，需首先向 CA 申请并安装数字证书，然后 Web 服务器才能支持 SSL 会话。在 IIS 中安装 SSL 分 5 个步骤：

- 生成证书请求文件。
- 提交数字证书申请。
- 下载证书文件。
- 在 IIS 服务器上导入并安装证书。
- 配置身份验证方式和 SSL 安全通道。

【问题 4】

略。（参见试题答案）

【问题 5】

略。（参见试题答案）

例题 7 答案

【问题 1】

（1）B 或 C （2）C 或 B

【问题 2】

（3）C （4）B

【问题 3】

（5）证书认证（颁发）机构 或 CA （6）B （7）A （8）C

【问题 4】

选中“要求安全通道（SSL）”复选框，选中“要求 128 位加密”复选框，选中“忽略客户端证书”单选按钮。

【问题 5】

（9）https:// 211.120.114.3: 8080

例题 8

某单位在部署计算机网络时采用了一款硬件防火墙，该防火墙带有三个以太网络接

口，其网络拓扑如图 15-10 所示。

【问题 1】

防火墙包过滤规则的默认策略为拒绝，表 15-5 给出防火墙的包过滤规则配置。若要求内部所有主机能使用 IE 浏览器访问外部 IP 地址 202.117.118.23 的 Web 服务器，为表中（1）～（4）空缺处选择正确答案，填写在答题纸相应位置。

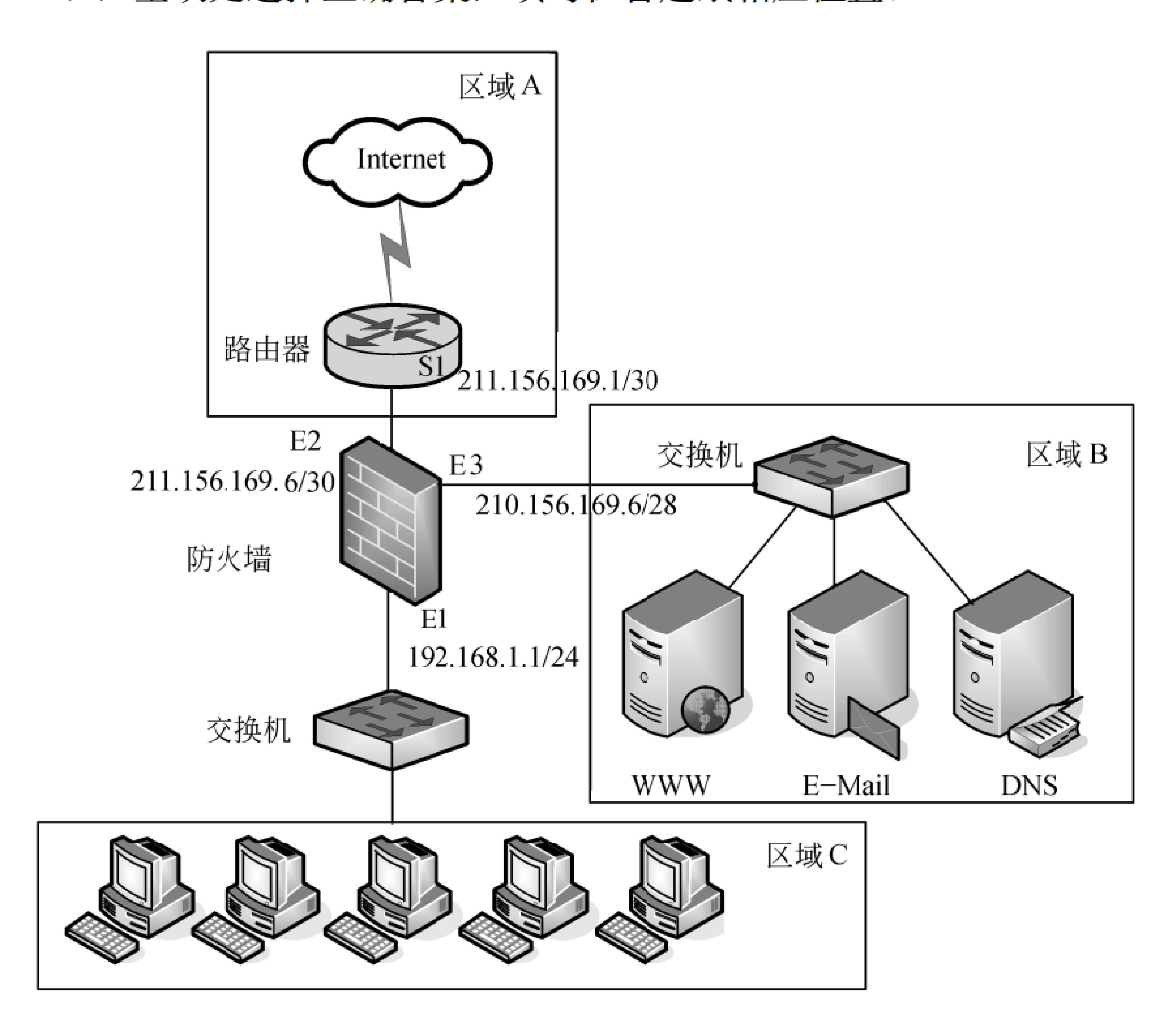


图 15-10　网络拓扑结构示意图

（1）备选答案：A．允许　B．拒绝

（2）备选答案：A．192.168.1.0/24　B．211.156.169.6/30　C．202.117.118.23/24

（3）备选答案：A．TCP　B．UDP　C．ICMP

（4）备选答案：A．E3→E2　B．E1→E3　C．E1→E2

表 15-5　防火墙的包过滤规则

序号	策略	源地址	源端口	目的地址	目的端口	协议	方向
1	（1）	（2）	Any	202.117.118.23	80	（3）	（4）

【问题 2】

内部网络经由防火墙采用 NAT 方式与外部网络通信，表 15-6 中（5）～（7）空缺

处选择正确答案，填写在答题纸相应位置。

表 15-6 防火墙的规则

源地址	源端口	目的地址	协议	转换接口	转换后地址
192.168.1.0/24	Any	（5）	80	（6）	（7）

（5）备选答案：A. 192.168.1.0/24　　B. any
C. 202.117.118.23/24

（6）备选答案：A. E1　　B. E2　　C. E3

（7）备选答案：A. 192.168.1.1　　B. 210.156.169.6　　C. 211.156.169.6

【问题 3】

图 15-10 中 （8） 适合设置为 DMZ 区。

（8）备选答案：A. 区域 A　　B. 区域 B　　C. 区域 C

【问题 4】

防火墙上的配置信息如图 15-11 所示。要求启动 HTTP 代理服务，通过 HTTP 缓存提高浏览速度，代理服务端口为 3128，要使主机 PC1 使用 HTTP 代理服务，其中“地址”栏中的内容应填写为 （9） ，“端口”栏中内容应填写为 （10） 。

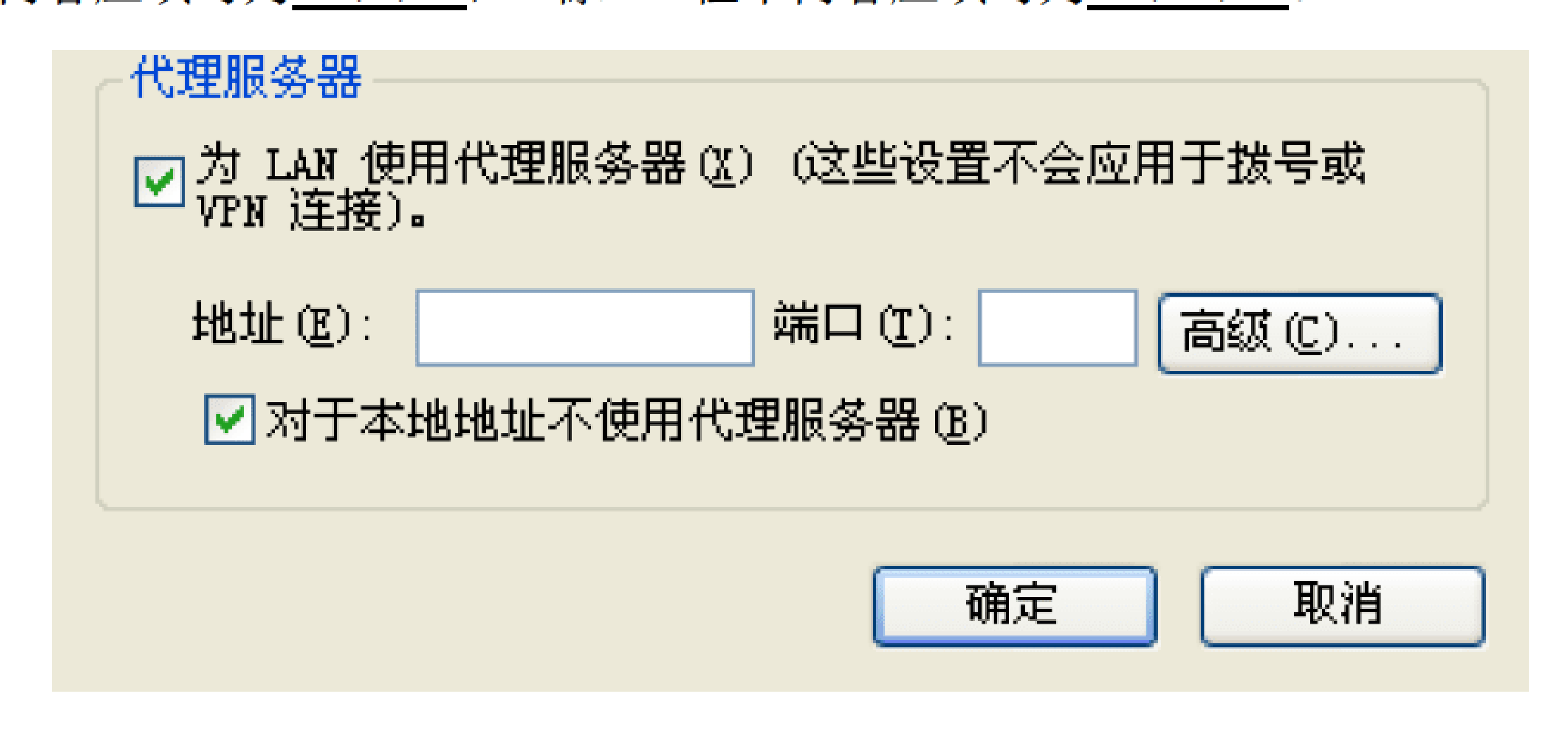


图 15-11 防火墙配置示意图

【问题 5】

NAT 和 HTTP 代理分别工作在 （11） 和 （12） 。

（11）备选答案：A. 网络层　　B. 应用层　　C. 服务层

（12）备选答案：A. 网络层　　B. 应用层　　C. 服务层

例题 8 分析

【问题 1】

由于防火墙包过滤规则的默认策略为拒绝，因此就需要对每个允许的网络通信操作

配置一条策略为“允许”的访问规则，即（1）应该选择答案 A（允许）。

根据题意，要使“内部所有主机能使用 IE 浏览器访问外部 IP 地址 202.117.118.23 的 Web 服务器”，并设置好了目的地址和目的端口。其中内部所有主机显然是指区域 C 中的所有主机，因此是 192.168.1.0 网络，即（2）应该选择答案 A（192.168.1.0/24）；而访问 Web 服务器将使用 HTTP 协议，HTTP 协议是基于 TCP 的，因此（3）应该选择答案 A（TCP），而方向的源端显然是 E1，而根据目标 IP 地址可知，它应该位于区域 A，因此目标端应该是 E2，因此（4）应该选择答案 C（E1→E2）。

【问题 2】

根据题意，内部网络（即 192.168.1.0/24 网络）经由防火墙采用 NAT 方式与外部网络通信。因此在访问任何外部主机时都需要进行 NAT 转换，即（5）应该选择 B（any）；而 NAT 转换都是在与外部连接的端口上进行的，即 E2，因此（6）应该选择 B；这一转换显然是将源 IP 地址替换成防火墙 E2 端口的 IP 地址，因此（7）应该选择 C，即 211.156.169.6。

【问题 3】

DMZ 网络通常较小，处于 Internet 和内部网络之间，一般情况下，配置成使用 Internet 和内部网络系统对其访问会受限制的系统，例如堡垒主机、信息服务器、Modem 组以及其他公用服务器。

而对于图 15-10 所示的网络而言，区域 A 显然是 Internet 网络，区域 C 是内部网络，因此适合设置为 DMZ 区的就是区域 B。

【问题 4】

对于代理服务器设置而言，IP 地址就是代理服务器的 IP 地址，在本例中就是防火墙的 IP 地址，即 192.168.1.1，而其端口号就是题意指定的代理服务端口 3128。

【问题 5】

NAT，网络地址转换，就是指在一个网络内部，根据需要可以随意自定义的 IP 地址，而不需要经过申请合法 IP 地址。在网络内部，各计算机间通过内部的 IP 地址进行通信。而当内部的计算机要与外部 Internet 网络进行通信时，具有 NAT 功能的设备（如路由器）负责将其内部的 IP 地址转换为合法的 IP 地址（即经过申请的 IP 地址）进行通信。

NAT 的应用场景主要是两种：一是从安全角度考虑，不想让外部网络用户了解自己的网络结构和内部网络地址；二是从 IP 地址资源角度考虑，当内部网络人数太多时，可以通过 NAT 实现多台共用一个合法 IP 访问 Internet。

在图 15-12 中展现了静态 NAT 的工作原理，从中不难看出它是对 IP 包进行操作，因此是工作在网络层。

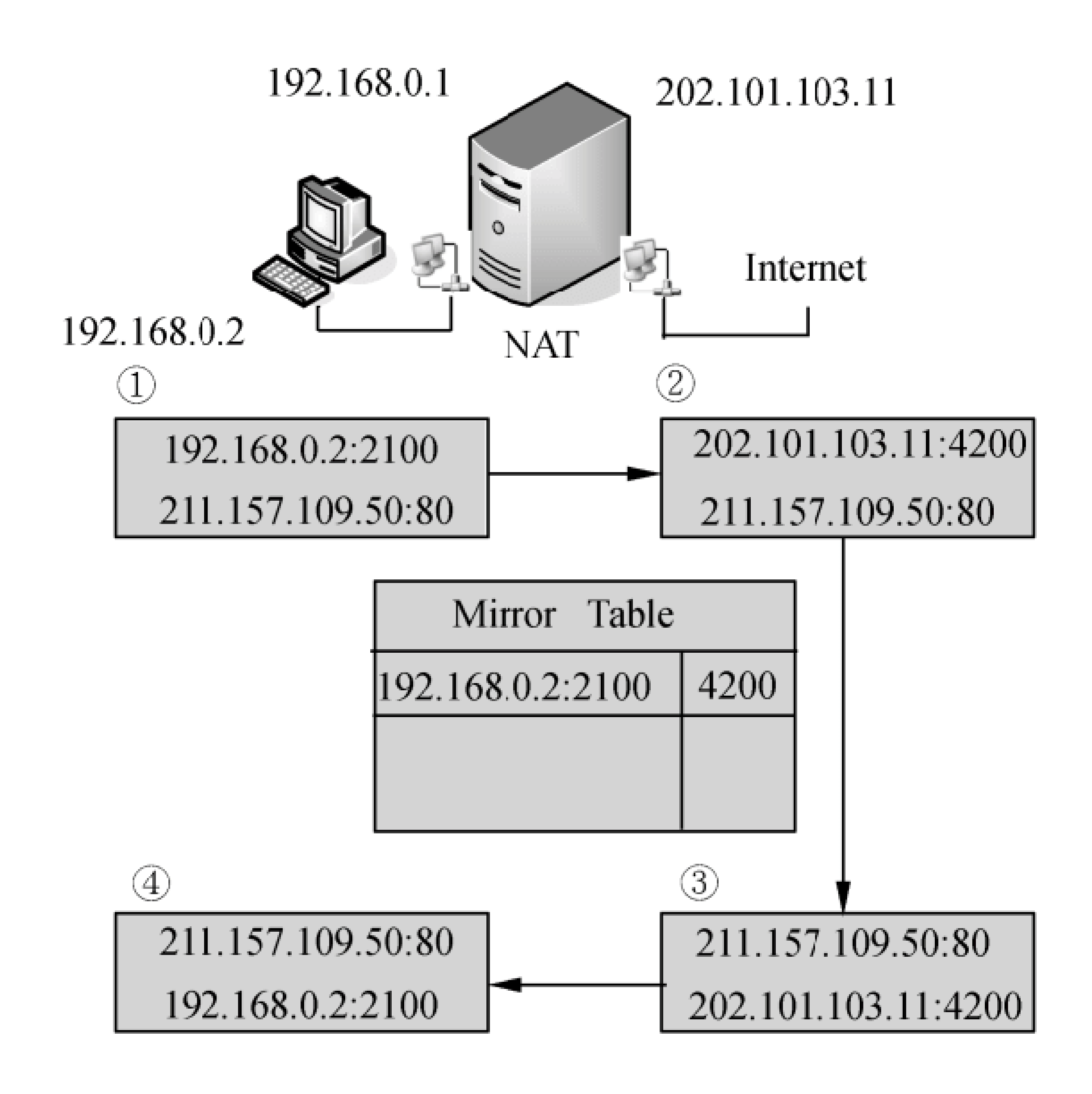
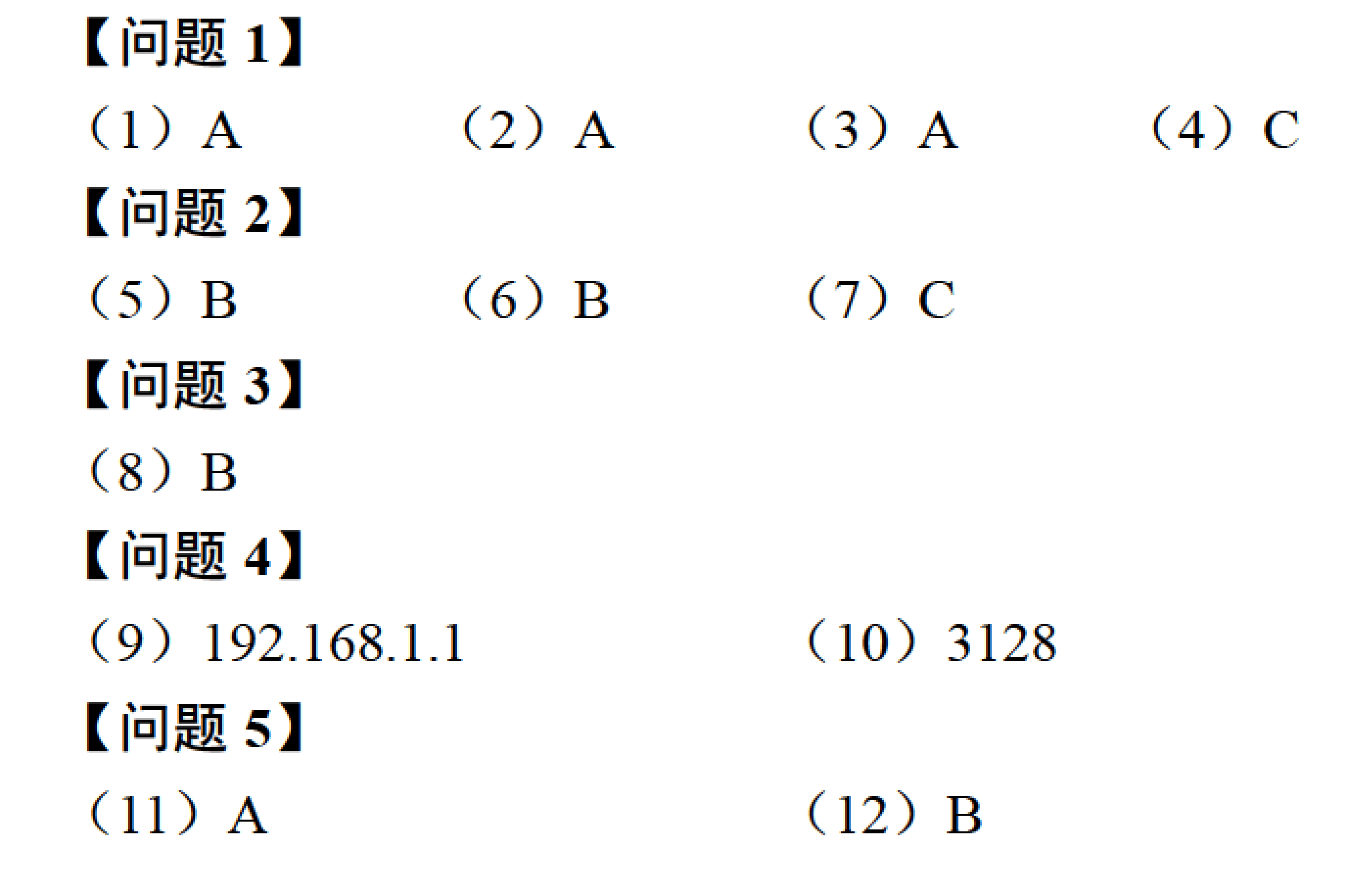


图 15-12 静态 NAT 工作原理示意图

而代理服务器的功能就是代理网络用户去获取网络信息。形象地说：它是网络信息的中转站。代理服务器能够让没有公网 IP 地址的计算机使用其代理功能高速、安全地访问互联网资源。当代理服务器客户端发出一个对外的资源访问请求时，该请求先被代理服务器识别并由代理服务器代为向外请求资源。由于一般代理服务器拥有较大的带宽、较高的性能，并且能够智能地缓存已浏览或未浏览的网站内容，因此在一定情况下，客户端通过代理服务器能够更快速地访问网络资源。从上面的描述中也不难发现，它是工作在应用层的。



例题 8 答案

【问题 1】

（1）A （2）A （3）A （4）C

【问题 2】

（5）B （6）B （7）C

【问题 3】

（8）B

【问题 4】

（9）192.168.1.1 （10）3128

【问题 5】

（11）A （12）B

第 16 章　计算机应用

计算机应用基础知识是网络管理员考试的一个重点，占上午考试的 7 分左右。主要考查 Windows 系统的基本操作、文字处理软件的使用、电子邮件和上网的一些基本知识。

16.1　Windows 基本操作

在 Windows 系统的基本操作方面，主要考查公共操作和文件操作。

16.1.1　公共操作

在 Windows 系统中，每个 Windows 窗口的右上角都有四个常用的操作按钮，分别是最小化按钮（）、最大化按钮（）、关闭按钮（）和还原按钮（）。

在 Windows 系统中，无论用户以什么形式、打开多少个窗口，仅有一个窗口是处于激活状态的。

在 Windows 系统中，剪切（Ctrl+X）、粘贴（Ctrl+V）、复制（Ctrl+C）操作都是基于剪贴板来实现的，它是暂存操作对象的内存缓冲区。其中复制-粘贴操作用来复制某部分信息，剪切-粘贴操作用来移动某部分信息。这两种操作都需要先选择要操作的信息，然后再通过菜单、快捷键等任意一种方式来执行复制或剪切操作，最后再执行粘贴或选择性粘贴操作。

在 Windows 系统中，可以安装多种汉字输入方法，并且其切换快捷键也是可以用户自定义的。

在 Windows 系统中，可以使用事件查看器来浏览日志文件，其中包含有应用程序日志、安全性日志、系统日志和 Internet Explorer 日志，如图 16-1 所示。

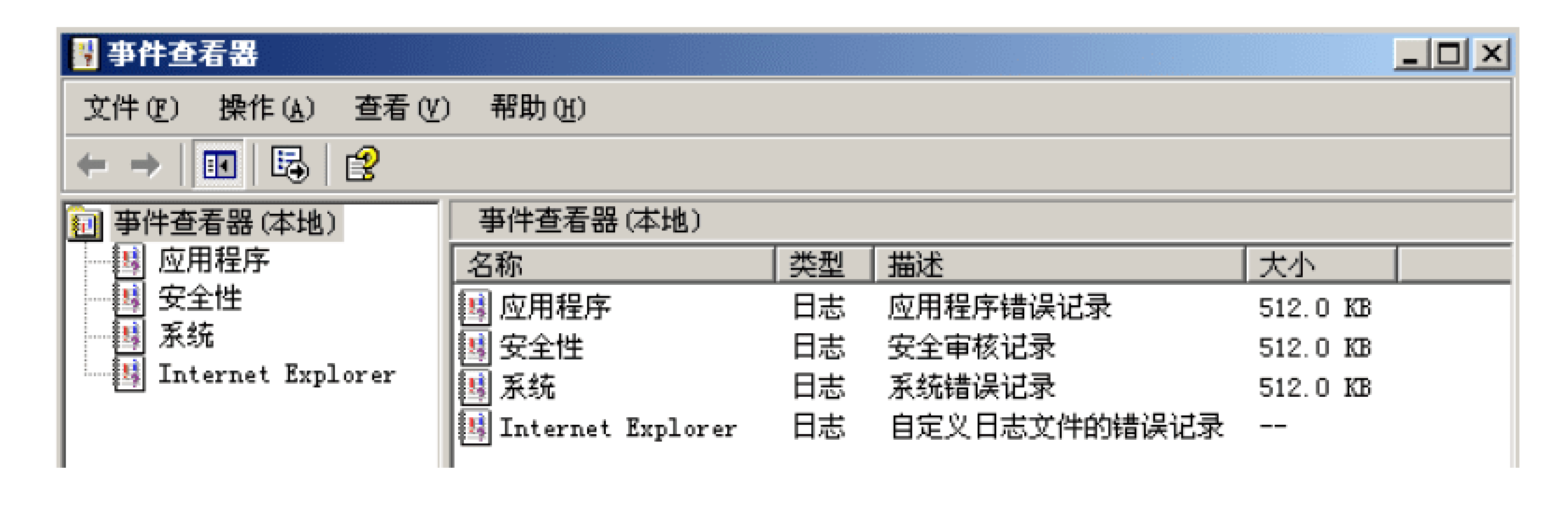


图 16-1　事件查看器

16.1.2 文件操作

Windows 系统中文件名长度不限，允许使用空格符，但不允许使用“\”、“?”、“:”、“"”、“<”和“>”等特殊字符。在 Windows 系统中，一个文件名中包含文件名和扩展名，扩展名中允许使用多个圆点。例如 csai.cn.exe 也是一个合法的文件名。

1．文件夹

在 Windows 系统中，采用多级树型目录结构，要唯一标识一个文件，必须指出所在盘符（也称为驱动器号）和路径名，因为不同目录下的文件可以同名（文件名和扩展名完全相同），但同一个目录下的文件不能同名。

针对 Windows 系统开发的许多软件不仅会创建自己的文件夹，还经常会在系统目录下放置动态链接库文件或其他系统文件，在注册表中添加自己的信息等，因此只删除应用程序文件夹通常是无法彻底卸载的。

在资源管理器中，单击窗口的“查看”菜单，弹出下拉菜单后，单击“图标”、“列表”或“详细资料”菜单项中的一个，则按相应的方式显示窗口中的文件和文件夹。当窗口内的文件、文件夹按“详细资料”方式显示时，每个文件和文件夹的信息包括名称、大小、类型、修改时间等。当单击每个项目名称时，将会以其为关键字进行排序。而在“图标”、“列表”方式都只列出文件名。

2．删除文件

Windows 中允许用户删除磁盘上的文件或文件夹，只需在“资源管理器”中操作的过程为：选中要删除的文件或文件夹，然后采用以下任一种方法进行删除，并在弹出的“删除确认”对话框中单击“是”按钮。

（1）按 Del 键：所选的文件将被删除，并存入回收站，可以恢复。

（2）右击打开快捷菜单，再选择“删除”命令，其后操作与按 DEL 键相同。

（3）按 Shift+Del 键：所选的文件将被彻底删除，不存入回收站，不能恢复。

（4）将文件拖到“回收站”，其作用与按 Del 键相同。

要注意的是，Windows 系统安装时生成的 Documents and Settings、Winnt 和 System32 文件夹是不能随意更改的，因为它们是系统文件夹，操作系统需要它们才能正常启动。

Windows 中允许用户删除磁盘上的文件或文件夹，如果发生误删除，还可以从回收站中将其恢复。回收站将占用硬盘的空间，每个分区都会有一个回收站所使用的目录。如果被删除的文件被存入回收站，则可以双击回收站图标，这将列出所有可恢复的文件或文件夹，选中要恢复的文件或文件夹，然后执行“还原”命令即可。

Windows 操作系统中，以下项目没有存储在回收站中且不能被还原（恢复）：

（1）从网络位置删除的项目。

（2）从可移动媒体（例如软盘、U 盘）删除的项目。

（3）超过回收站存储容量的项目。

（4）在回收站中被清空的项目。

3．文件属性

Windows 的文件和文件夹都有自己的属性，用户也可以重新设置它们的属性。这些属性主要包括四种：

（1）只读：只能使用（读取），不能被修改。

（2）隐藏：在默认情况下，资源管理器不会列出隐藏文件。

（3）存档：是指该文件或文件夹是否能备份，设置了存档属性说明其可以备份。

（4）系统：是指该文件或文件夹由系统控制，不能够随意修改。

4．磁盘碎片

计算机系统在运行的过程中，会对磁盘上的文件进行插入、修改和删除，这样难免会在磁盘上形成“空洞”，即所谓的“碎片”，使得文件可能会存放在不连续的空间中，影响文件的存取速度。如果通过整理磁盘碎片，将文件存放在连续的空间中，并将“碎片”连接起来形成一个大的空闲区，可提高系统运行效率。所以，我们必须定期进行磁盘碎片的整理。

用户可以从“开始”菜单中选择“程序”→“附件”→“系统工具”→“磁盘碎片整理程序”，弹出选择驱动器窗口，选择要整理的分区，然后单击“确定”按钮即可开始整理。

还有一种方式可以进入磁盘碎片整理程序。例如，如果要整理 D 盘上的碎片，可选中 D 盘，单击鼠标右键，选择“属性”对话框中的“工具”选项卡，如图 16-2 所示。

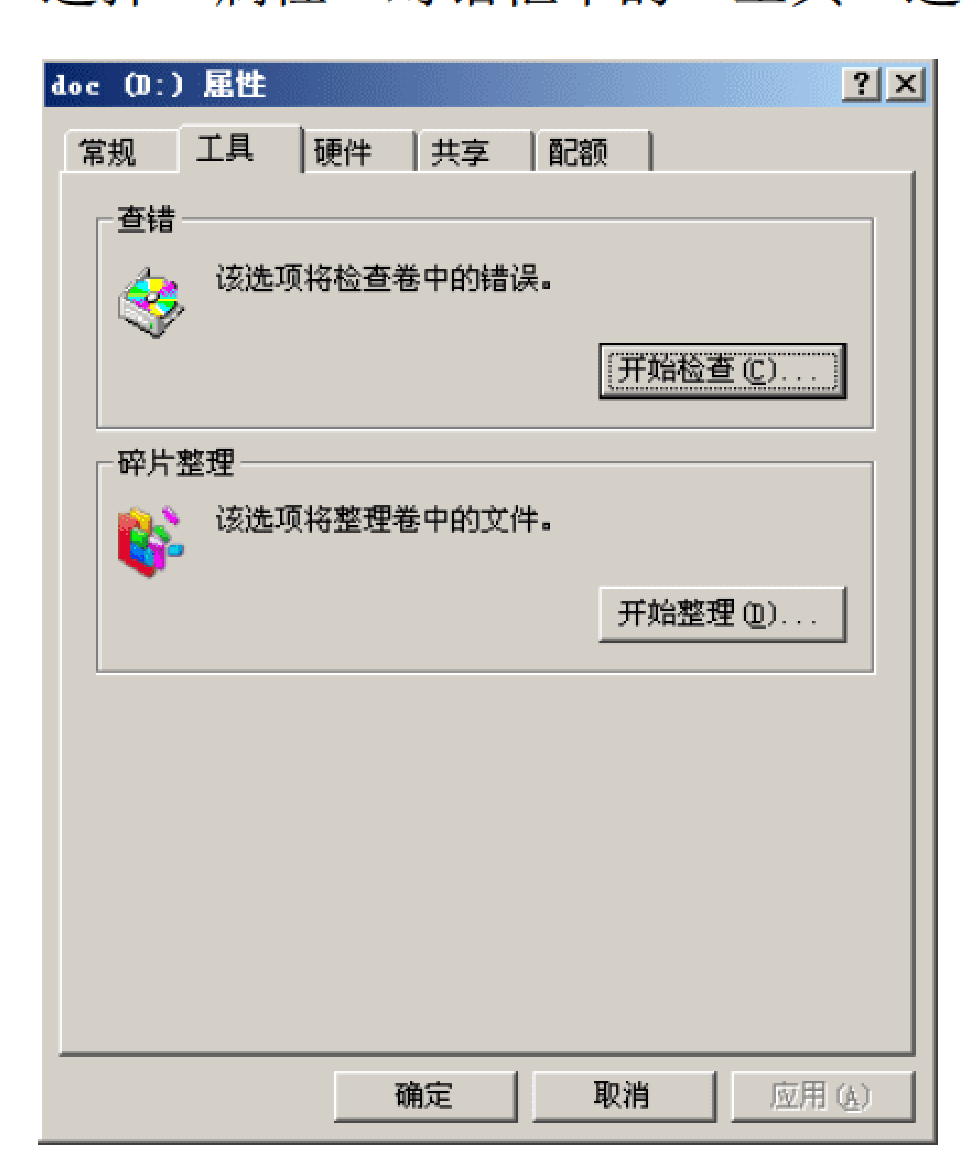


图 16-2　“属性”对话框中的“工具”选项卡

在图 16-2 中，单击“开始整理”按钮，就可启动磁盘碎片整理程序。磁盘碎片的整

理过程非常耗时，往往需要数个小时。

16.2 Word 基本操作

Microsoft Word 是微软公司的一个文字处理器应用程序。它最初是由 Richard Brodie 为了运行 DOS 的 IBM 计算机而在 1983 年编写的。随后的版本可运行于 Apple Macintosh（1984 年），SCO UNIX，和 Microsoft Windows （1989 年），并成为了 Microsoft Office 的一部分。使用 Microsoft Word 创建和编辑信件、报告、网页或电子邮件中的文本和图形。

Word 的菜单条和工具栏如图 16-3 所示。



图 16-3 Word 的菜单和工具栏

Word 编辑的文件的默认扩展名为 doc，也可以保存为 tif 格式的文件。

16.2.1 工具栏图标按钮

下面，我们围绕工具栏的图标，作些简单介绍。

：新建一个文档，相当于使用“文件”菜单的“新建”命令。

：打开一个文档。当单击这个按钮时，会打开一个“打开文档”的窗口，如图 16-4 所示。

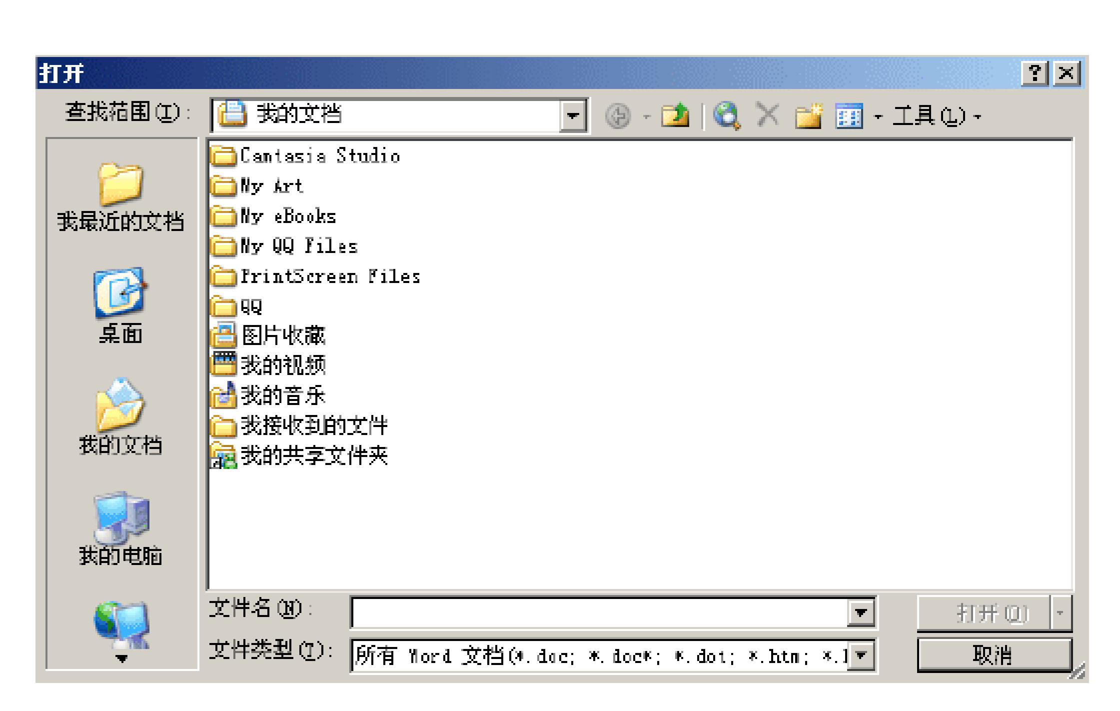


图 16-4 打开文档

：保存正在编辑的文件，单击这个按钮的效果与单击“文件”菜单中的“保存”命令效果是一样的。其快捷键为“Ctrl+S”。如果要把文件另外保存为一个名字，或者把文件保存到另外一个地方（不是文件当前所在的磁盘或目录），则需要选择“文件”菜单中的“另存为”按钮。此时，会打开“另存为”对话框，在对话框中选定要存盘的路径

并输入文件名，可将没有保存的文件保存。

：自由访问文档的权限设置。这是 Microsoft Office 2003 中的一个新增功能，每个作者可使用它为访问和使用文档或电子邮件的用户指定权限，并帮助防止未经授权的人员打印、转发或复制敏感信息。使用此项技术限制文档或邮件的权限后，无论信息在什么地方，都会施加访问和使用限制，这是因为访问电子邮件或文档的权限存储在文件本身中。

：把正在编辑的文件作为电子邮件发送出去。如果单击该按钮，则会启动 Outlook。

：打印正在编辑的文档。在 Word 中要执行打印当前页、打印文档全文、弹出打印对话框进行设置操作，都可以通过单击该按钮，然后在弹出的对话框中选择相应的功能来实现。

：打印预览，把打印的结果在屏幕上显示，而不执行实际的打印。例如，图 16-5 就是一个打印预的窗口。

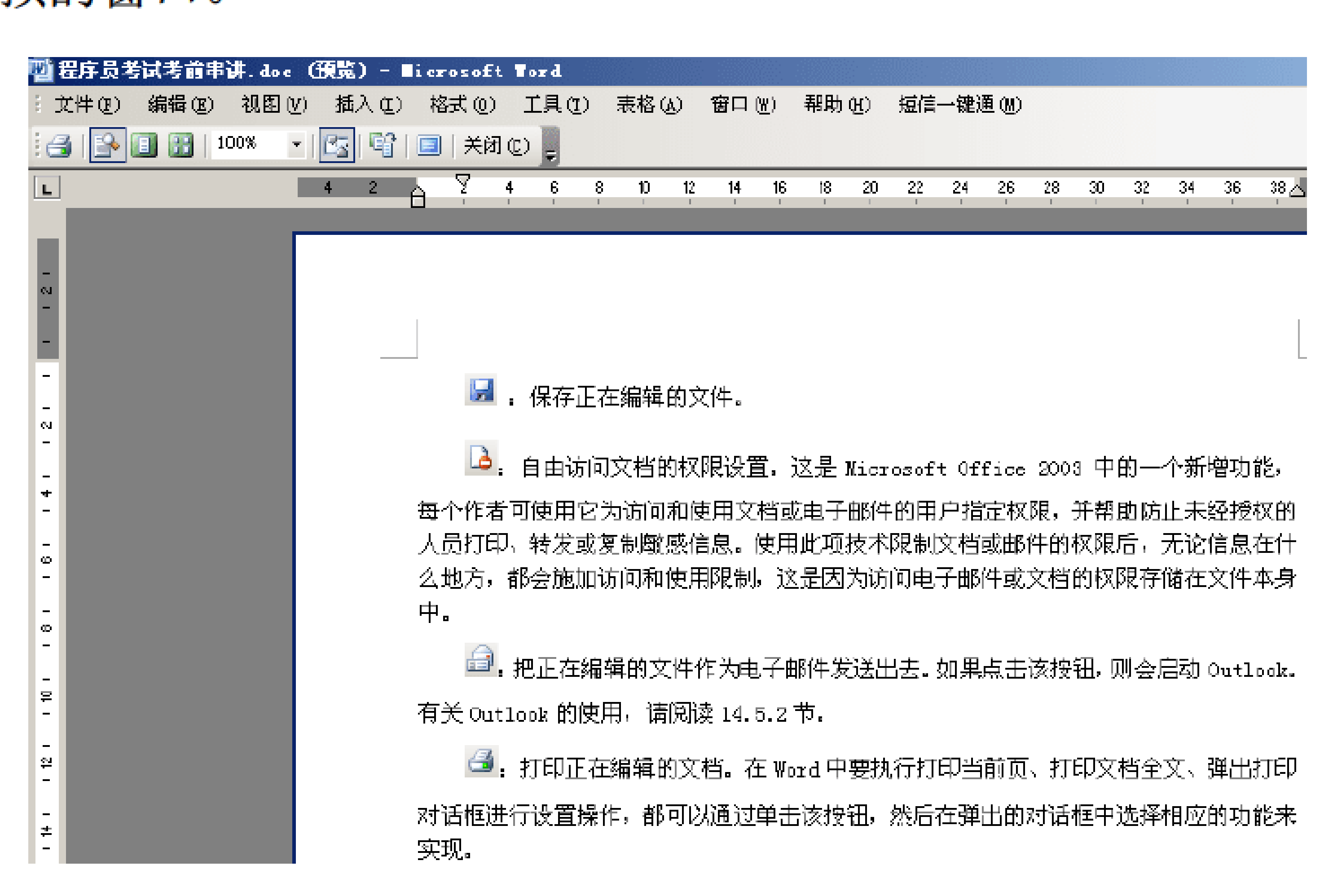


图 16-5　打印预览窗口

在“打印预览”方式下，单击“关闭”按钮即可返回编辑状态。“打印预览”、“放大镜”和“全屏显示”均为在预览状况下的操作。

：粘贴。

：剪切。

：复制。

以上三个按钮的含义与 16.1.1 节中的操作是一样的。

：格式刷。当选定某些文字或段落后，单击该按钮，然后再去选择一些文字或段落，则会把前面选定文字的格式（包括字体、字型、行间距、段间距等）应用到后面选定的文字上。

：撤销操作，也就是撤销当前进行的操作。在 Word 中记录了用户的每个操作步

骤，如果发生错误，可以进行多次撤销。

：恢复操作。这是撤销操作的反操作，也就是把撤销的操作又恢复过来。

：在文档中插入超链接，用鼠标单击该链接时，则可以连接到相应的网页。

：表格工具，对表格进行操作，表格增加行、列，删除行、列，以及画各种线条等。

：在文档中插入表格，用户可以自由选择表格的行数和列数。

：在文档中插入 Excel 表格。有关 Excel 的使用，请阅读 16.4 节。

16.2.2 其他功能

本节介绍如何选择内容、查找和替换操作，以及表格的基本操作。

1．选择内容

在文档操作前，首先要指明操作的对象。这就需要选择文档。选择的方法主要有三种：鼠标、F8 键 Shift+光标。

在被选择内容的开始位置按下鼠标左键不松开，将鼠标拖到被选择内容的结束位置，然后再松开鼠标左键。此时，鼠标始点和终点之间的文档内容就将被选中。鼠标法还有其他的一些用法：

（1）将鼠标光标移动待选句子的任意一个字符上，双击鼠标右键，两个标点之间的内容将被选中。

（2）将鼠标移动被选句子上，按住 Ctrl 键，单击鼠标左键，则鼠标所在的句子被选中，即选择了用句号分割的一个句子。

（3）将鼠标移到某一行的左侧空白处，当鼠标变为指向右上方向的箭头后，单击鼠标左键，便选定了该行的全部内容。

（4）将鼠标移到某一段落的左侧空白处，当鼠标变为指向右上方向的箭头后，双击鼠标左键，便选定了该段的全部内容。

（5）将鼠标移动要选择的矩形区域的一个角上，然后按下 Alt 键不放，再按下鼠标左键不放，拖到矩形的另一个对角上，然后放开鼠标键再放开 Alt 键，则以该对角线的矩形区域被选中。

（6）将鼠标移动文档左边空白区内任意处，当鼠标变为指向右上方向的箭头后，连击三次鼠标左键，将选中全部文本。

选中后，可以采用以下两种方法之一将文档的内容复制到同一个文档内：一是鼠标法，它的操作与移动相似，区别在于在“按下鼠标左键”的同时，还需要按下 Ctrl 键，松开时同时松开；二是用剪贴板方法，其操作类似。

如果先将鼠标移动已选中的内容上；按下鼠标左键不放，拖到目的位置；放开鼠标左键，则将完成移动操作。

2．查找和替换

在文档编辑过程中，一次要对多个字符进行更改的可以采用“查找/替换”的方法。例如，如果想把文中所有的“希赛网”替换成“学赛网”，可以使用替换来做。打开“编辑”菜单，单击“替换”命令，就出现这样一个“查找和替换”对话框的“替换”选项卡，如图 16-6 所示。



图 16-6　查找与替换

在图 16-6 中，在“查找内容”文本框中输入要替换的内容“希赛网”，在下面输入要替换成的内容“学赛网”，单击“查找下一处”按钮，Word 就自动在文档中找到下一处使用这个词的地方，这时单击“替换”按钮，Word 会把选中的词替换掉并自动选中下一个词。如果确定了文档中这个词肯定都要被替换掉，那就直接单击“全部替换”按钮，完成后 Word 会告诉替换的结果。

查找时也采用模糊查找，使用通配符。通配符是一个键盘字符，例如“*” 或“?”，当查找某些内容时，我们可以使用它来代替一个或多个真正字符。当我们不知道真正字符或者不想键入完整名字时，常常使用通配符代替一个或多个字符。

3．拼写错误识别

在 Word 编辑状态下，有些英文单词和汉字下面会自动加上红色或绿色的波浪型细下划线。波浪型细下划线提醒用户此处可能有拼写或语法错误，为红色表示可能是拼写问题，为绿色可能是语法问题；波浪型细下划线不属于文档内容，打印文档时不会被打印出来。

4．表格操作

在 Word 中，“表格”菜单中的“删除列”命令将会删除当前选择的所有表格列，“删除行”命令将会删除当前选择的所有表格行。要注意的是，如果先选择表格中的一行，然后单击“删除列”命令，则将删除表格中的所有列，也就意味着整个表格将被删除。同样，如果先选择表格中的一列，然后单击“删除行”命令，也将删除整个表格。

选择了多个列以后，然后单击“表格”菜单中的“自动调整”中的“平均分布各列”，则会把所选择的列的宽度设置为全部相等。同样，如果选择了多个行以后，然后单击“表格”菜单中的“自动调整”中的“平均分布各行”命令，则会把所选择的行的高度设置为全部相等。

先选中一行单元格，打开“表格”菜单，单击“合并单元格”命令，则把选中的单元格合并成一个单元格。先选中一列单元格，打开“表格”菜单，单击“合并单元格”命令，选中的这些单元格也就合并成一个单元格。

选取单元格，打开“表格”菜单，单击“拆分单元格”命令，弹出“拆分单元格”对话框，选择拆分成行和列的数目，单击“确定”按钮，这样就可以拆分单元格。也可以在单元格中单击鼠标右键，在打开的快捷菜单中选择“拆分单元格”命令，或者单击“表格和边框”工具栏上的“拆分单元格”按钮，可以打开“拆分单元格”对话框。

5．选项操作

如果要在 Word 中设置一些个性化的选项，则可单击“工具”菜单中的“选项”命令，该菜单项中提供了大量可配置的选项，包括视图、常规、编辑、打印、保存、安全性（其中包括打开权限密码）、拼写和语法、修订、用户信息、兼容性、中文版式、文件位置等，如图 16-7 所示。

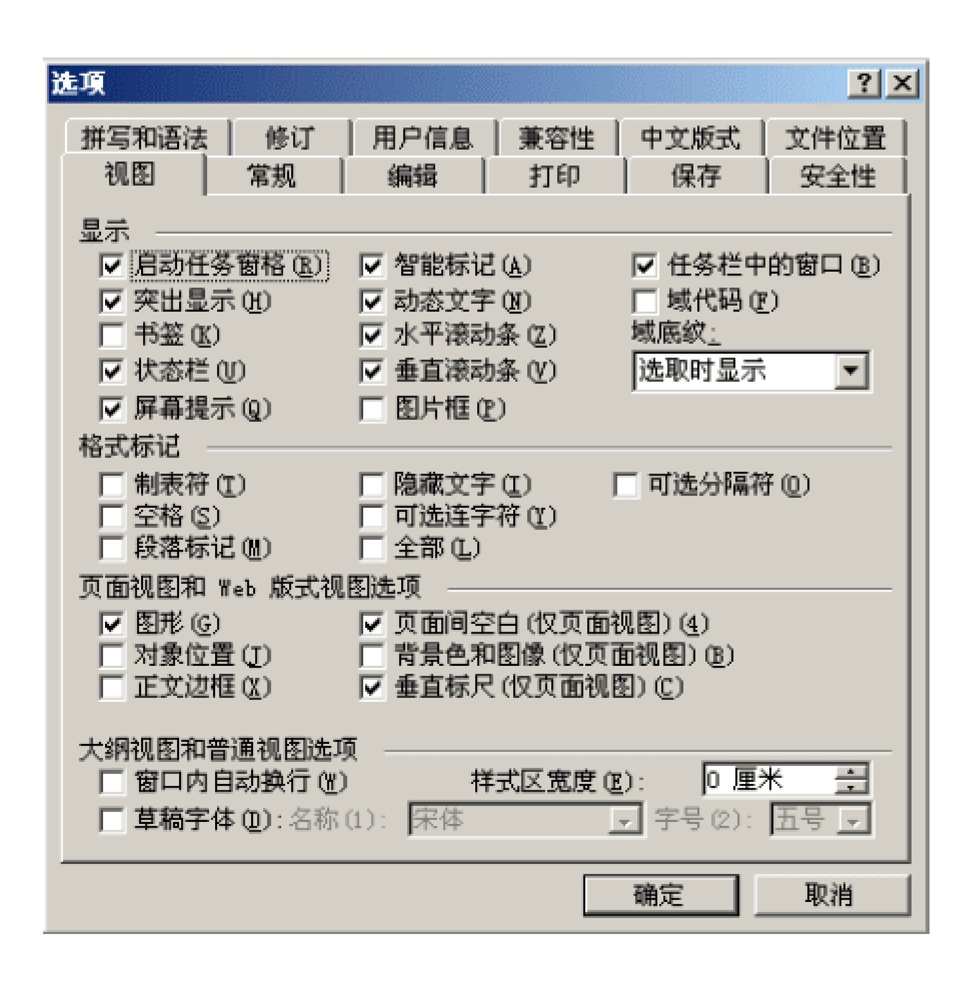


图 16-7　选项设置

16.3　Excel 基本操作

Excel 是微软公司出品的 Office 系列办公软件中的一个组件，确切地说，它是一个电子表格软件，可以用来制作电子表格、完成许多复杂的数据运算，进行数据的分析和预测并且具有强大的制作图表的功能，现在的新版本 Excel 2000 还可以制作网页。

Excel 工作簿中可以包含多个工作表，每个工作表包括多个行、每一行中也有多个列，而最小的组成单位应该是单元格。

（1）工作簿：一个 Excel 文件，一个工作簿中最多可以有 255 个工作表。

（2）工作表：工作簿中的一张表格，系统默认有 3 个工作表，表名为 sheet1、sheet2、

sheet3，一张工作表由 65 536 个行、256 个列组成。

（3）单元格：Excel 的基本操作单位，数据都保存在单元格中，每个单元格都有唯一的地址，地址格式为“表名！列号行号”，例如，“Sheet2!A3”表示工作表 Sheet2 的第 A 列第 3 行的那个单元格。

Excel 的界面如图 16-8 所示。

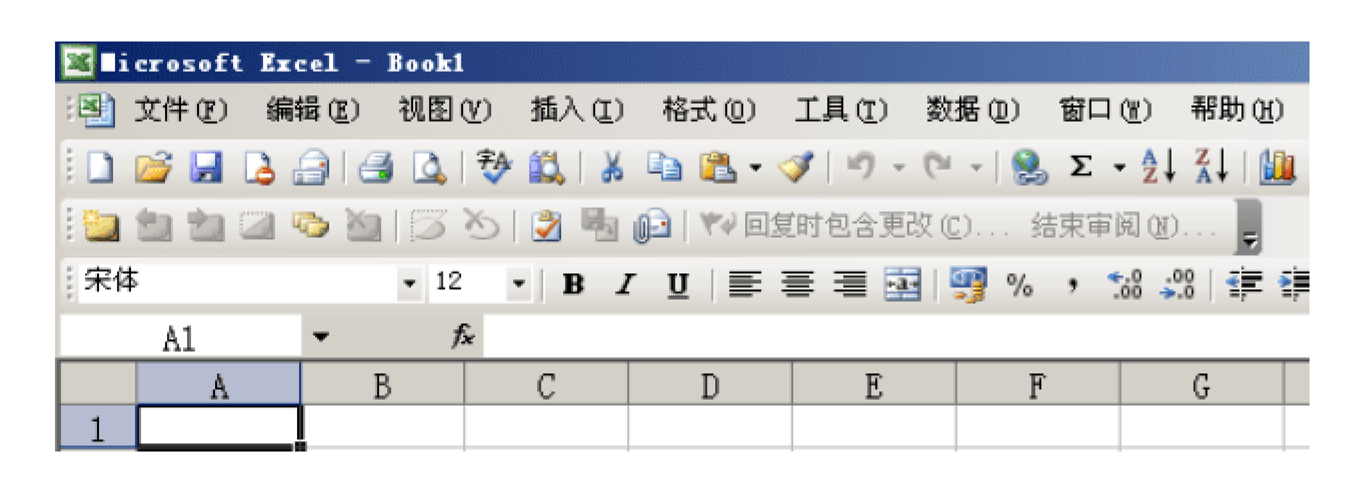


图 16-8　Excel 界面图

从图 16-8 可以看出，Excel 的菜单和工具栏与 Word 的是相似的，因此，我们不再一一介绍。在 Windows 系统中，相同的图标所代表的含义是相同的。

在图 16-8 中，有四个图标是 Word 没有的，分别介绍如下：

Σ：自动求和，对所选择的列的数据求和，并把结果显示在该列的最后一行。

：升序排序，对所选择的内容按照关键字进行从小到大的排序。

：降序排序，对所选择的内容按照关键字进行从大到小的排序。

：图表向导，单击该按钮，将打开一个图表向导，该向导会根据 Excel 表中的数据生成各种形式的图形，如图 16-9 所示。



图 16-9　图表向导

Excel 具有自动填充功能，例如，当我们在 A1 和 A2 两个单元格中分别输入值 2 和

2.5 后，就规定了自动填充的等差数列规则，当选择 A1:A2 区域后再将鼠标指针放在该区域右下角填充柄上，向下拖动时就将开始按这个等差数列规则进行填充，因此 A3 的值就是 3，A4 的值是 3.5，……，依此类推 A10 的值就是 6.5。

又如，如果我们在 B1 和 B2 两个单元格中分别输入“星期一”和“星期二”，当选择 B1:B2 区域后再将鼠标指针放在该区域右下角填充柄上，向下拖动时，B3 的值就是“星期三”，B4 的值是“星期四”，……，依此类推 B7 的值就是“星期日”。

在 Excel 中，默认的单元格引用为相对引用，如 A1、B3 等。相对引用是当公式在复制或移动时，系统会根据移动的位置自动调节公式中引用单元格的地址。例如，在图 16-10 中，若在 C1 中输入公式“=A1+B1”，则 C1 的结果为 102；若将公式复制到 C2，用户会发现 C2 中的值是 104，编辑栏中显示公式为“=A2+B2”。也就是说相对地址发生了变化。

	A	B	C
1	101	1	
2	102	2	
3			

图 16-10 单元格引用

如果在行号和列号前均加“＄”符号，则代表绝对引用。公式复制时，绝对引用单元格将不随公式位置变化而改变。如果在图 16-10 中，C1 公式改为“=＄A＄1+＄B＄1”，再将公式复制到 C2，C2 的值仍为 102，公式也仍为“=＄A＄1+＄B＄1”。

在具体的文字编辑上，例如保存、复制和粘贴、保存、查找和替换等，Excel 的操作与 Word 的操作是相同的，限于篇幅，在此不作详细介绍。

16.4 上网基础操作

在上网基础操作方面，我们主要掌握 IE 和 Outlook 软件的使用，以及如何才能不感染病毒和木马，如何保证系统的安全这样问题。

16.4.1 IE 的使用

Internet Explorer（IE）是微软公司推出的一款网页浏览器，是目前使用最广泛的网页浏览器。

1．基本界面

Internet Explorer 是微软的新版本 Windows 操作系统的一个组成部分。在旧版的操作系统上，它是独立且免费的。从 Windows 95 OSR2 开始，所有新版本的 Windows 操作系统附带浏览器。目前，最新的版本是 IE 8.0，其界面如图 16-11 所示。



图 16-11　IE 运行界面图

在图 16-11 中，白色方框中的“http://www.educity.cn/ruankao/kspx.htm”称为 URL，也就是我们要访问的网站的地址。相应地，这个方框就称为地址栏。如果在 URL 中不填写协议类型，则 IE 浏览器默认使用 HTTP 协议。

2．收藏夹

我们在上网时访问了大量的网站，但希望把一些经常要访问的网站记下来，不要每次都输入 URL 地址，就可以使用 IE 的收藏夹功能。将这些网站收藏进收藏夹，访问起来就方便了。当要访问时，就像使用窗口的菜单一样，直接单击就可以，如图 16-12 所示。

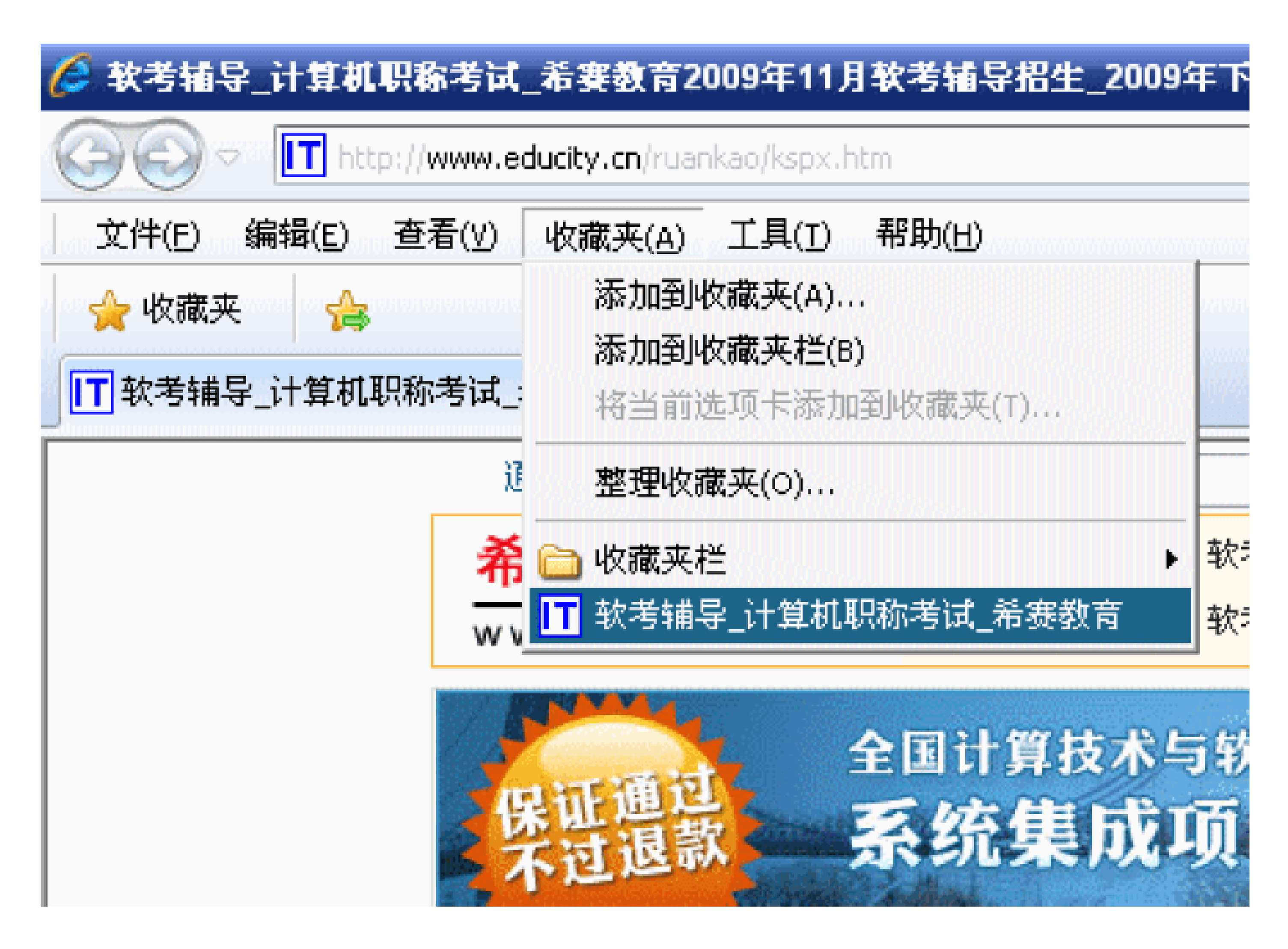


图 16-12　收藏夹功能

例如，如果我们把希赛教育网收藏到收藏夹，则我们需要再次访问希赛教育网时，只要单击“收藏夹”菜单，然后在下拉子菜单中单击“希赛教育网”就可以直接访问希赛教育网。

3．ActiveX 控件

在上网的过程中，由于 ActiveX 控件、脚本（例如 Java Script）可以嵌入到 HTML 页面中，并下载到浏览器端执行，会给浏览器端造成一定程序的安全威胁。而且还可以生成在客户端可执行的程序模块，这些都可能造成对系统的破坏。因此，可以使用 IE 菜单命令“工具”→“Internet 选项”→“安全”→“自定义级别”，将所有的与 ActiveX 控件相关的项，修改成为“提示”或“禁用”，如图 16-13 所示。

如果要禁用脚本则修改与脚本相关的项，使其为“提示”或“禁用”，如图 16-14 所示。

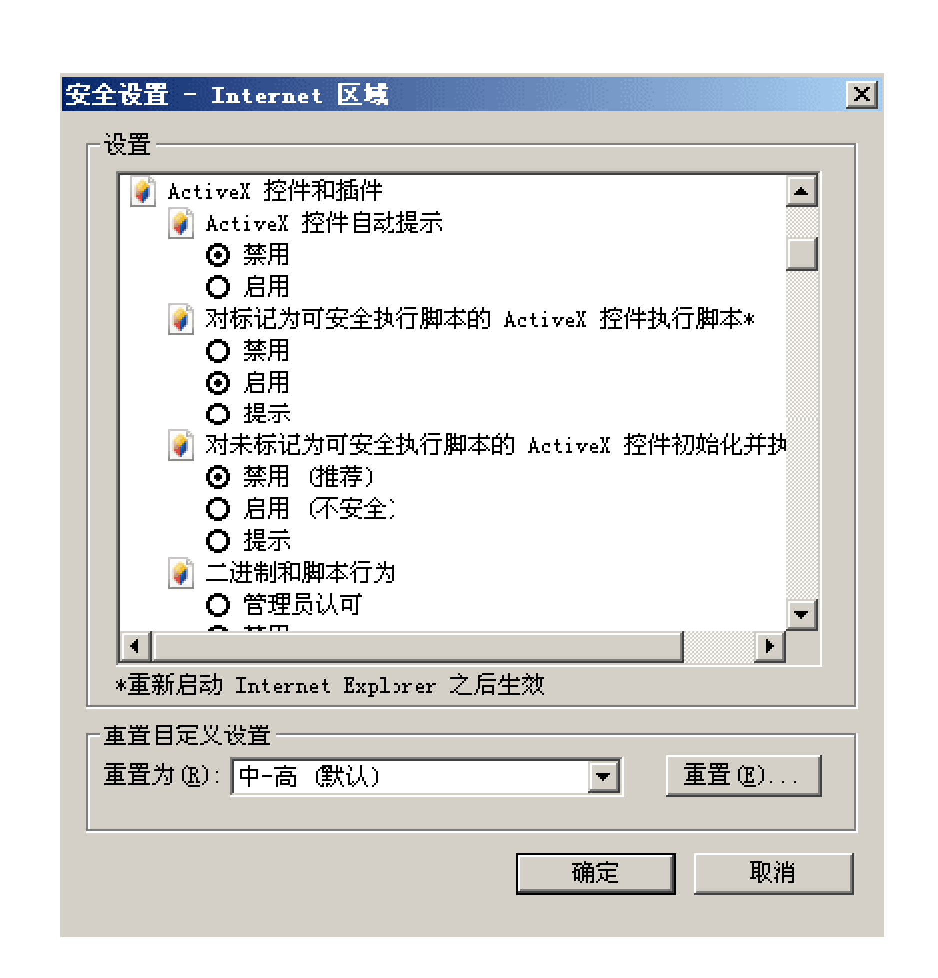



图 16-13 禁用 ActiveX 插件

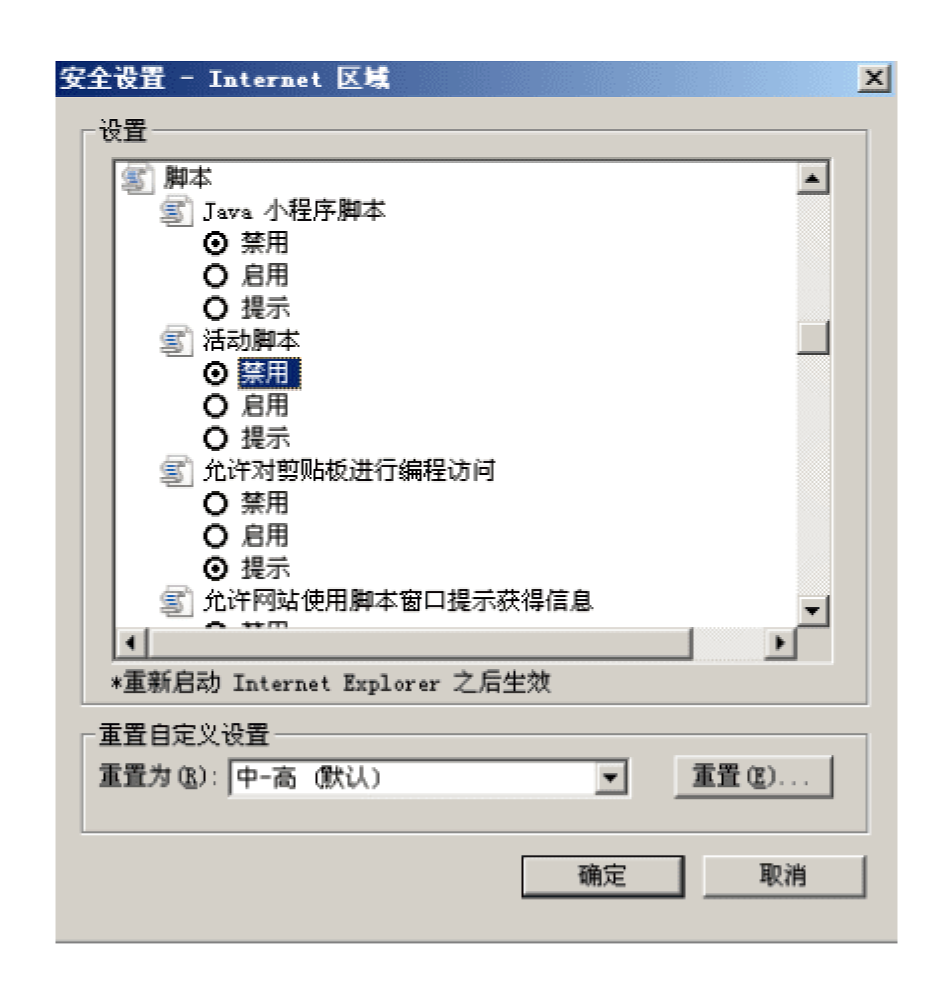


图 16-14 禁用脚本

其中“提示”是指当遇到 ActiveX 控件或脚本时，将提示用户，由用户决定是否使用。

4．Cookies 设置

Cookies 是一种能够让网站服务器把少量数据储存到客户端的硬盘或内存，或是从客户端的硬盘读取数据的技术。Cookies 是当我们浏览某网站时，由 Web 服务器置于硬盘上的一个非常小的文本文件，它可以记录我们的用户 ID、密码、浏览过的网页、停留的时间等信息。当我们再次来到该网站时，网站通过读取 Cookies，得知相关信息，就可以做出相应的动作，例如，我们不用输入 ID、密码就直接登录等。

从本质上讲，它可以看作是用户的身份证。但 Cookies 不能作为代码执行，也不会传送病毒，且为用户所专有，并只能由提供它的服务器来读取。保存的信息片段以“名/值”对的形式储存，一个“名/值”对仅仅是一条命名的数据。一个网站只能取得它放在

用户计算机中的信息，它无法从其他的 Cookies 文件中取得信息，也无法得到用户计算机上的其他任何东西。

Cookies 中的内容大多数经过了加密处理，因此一般用户看来只是一些毫无意义的字母数字组合，只有服务器的 CGI 处理程序才知道它们真正的含义。

由于 Cookies 是我们浏览的网站传输到用户计算机硬盘中的文本文件或内存中的数据，因此它在硬盘中存放的位置与使用的操作系统和浏览器密切相关。在 Windows 9X 系统计算机中，Cookies 文件的存放位置为 C:WindowsCookies，在 Windows NT/2000/XP 的计算机中，Cookies 文件的存放位置为 C:\Documents and Settings\用户名\Cookies。

我们可以在 IE 的“工具”→“Internet 选项”的“常规”选项卡中，选择“设置→查看文件”，查看所有保存到计算机里的 Cookies。硬盘中的 Cookies 文件可以被 Web 浏览器读取，它的命令格式为：用户名@网站地址[数字].txt。要注意的是：硬盘中的 Cookies 属于文本文件，不是程序。

我们可以对 Cookies 进行适当设置：打开“工具”→“Internet 选项”中的“隐私”选项卡，调整 Cookies 的安全级别。通常情况，可以调整到“中高”或者“高”的位置。多数的论坛站点需要使用 Cookies 信息，如果我们从来不去这些地方，可以将安全级调到“阻止所有 Cookies”。如果只是为了禁止个别网站的 Cookies，可以单击“编辑”按钮，将要屏蔽的网站添加到列表中。在“高级”按钮选项中，可以对第一方 Cookies 和第三方的 Cookies 进行设置，第一方 Cookies 是我们正在浏览的网站的 Cookies，第三方 Cookies 是非正在浏览的网站发给我们的 Cookies，通常要对第三方 Cookies 选择“拒绝”。如果需要保存 Cookies，可以使用 IE 的“导入导出”功能，选择“文件”→“导入导出”，按提示操作即可。

16.4.2　Outlook 的使用

Outlook 或 Outlook Express 是微软公司开发的一个电子邮件处理程序，一般集成在 Windows 操作系统中，其使用界面如图 16-15 所示。

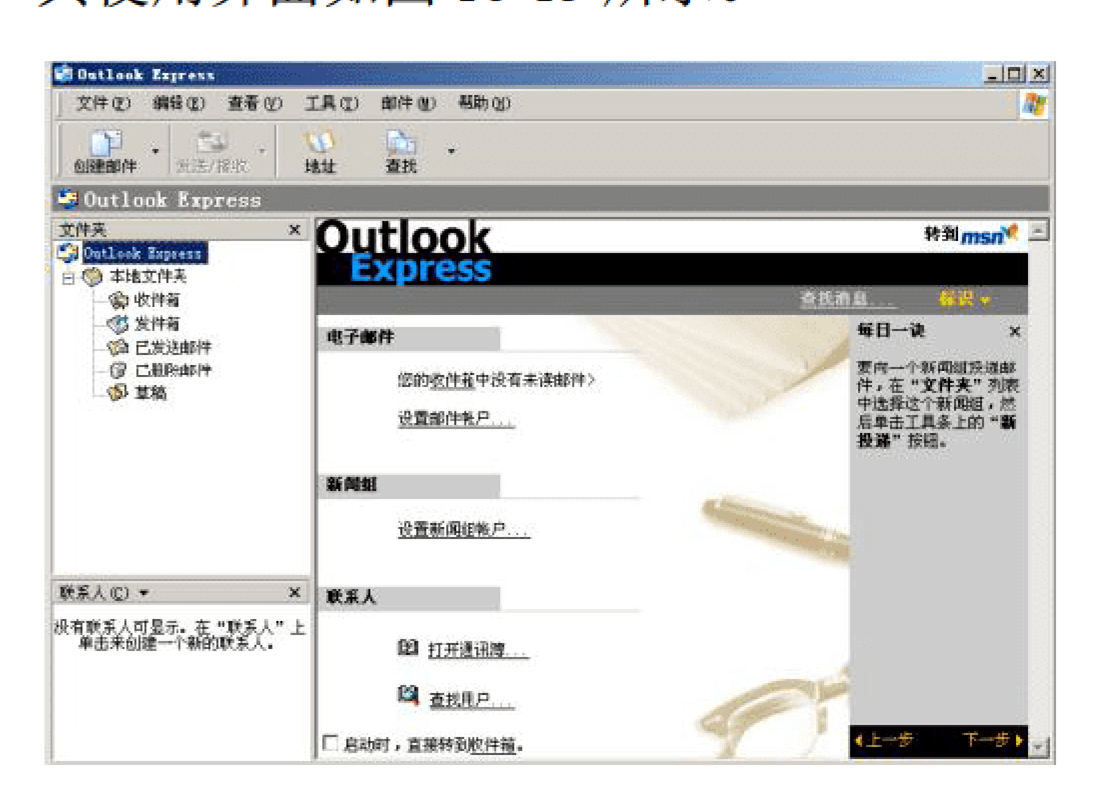


图 16-15　Outlook 界面

Outlook 是使用最广泛和最简单的电子邮件客户端软件之一，Outlook 通常采用 SMTP 和 POP3 来实现电子邮件的收发操作。附件是电子邮件系统中应用最灵活和最重要的功能，当邮件内容较大时，可将其先生成一个文件，然后再利用 Outlook 提供的附件功能进行传送。使用附件功能传送文件时，可以不受文件信息类型和格式的限制，如传输各种声音、图像等多媒体信息。采用附件功能传送文件，甚至还可以解决某些收发邮件时的乱码问题。

Outlook 不是电子邮箱的提供者，它是 Windows 操作系统的一个收、发、写、管理电子邮件的自带软件，即收、发、写、管理电子邮件的工具，使用它收发电子邮件十分方便。

通常我们在某个网站注册了自己的电子邮箱后，要收发电子邮件，须登录该网站，进入电邮网页，输入账户名和密码，然后进行电子邮件的收、发、写操作。例如，我们在希赛网注册电子邮箱 edu@csai.cn，则需要进入 http://mail.csai.cn，输入用户名 edu，然后再输入密码，就可以进入 Web 方式的邮件收发界面。

使用 Outlook 后，这些顺序便一步跳过。只要打开 Outlook 界面，Outlook 程序便自动与我们注册的网站电子邮箱服务器联机工作，收下电子邮件。发信时，可以使用 Outlook 创建新邮件，通过网站服务器联机发送。

另外，Outlook 在接收电子邮件时，会自动把发信人的电子邮件地址存入“通信簿”，供用户以后调用。还有，当我们单击网页中的电子邮件超链接时，（如希赛网页面最底下的“不良信息举报信箱”）会自动弹出写邮件的界面，该新邮件已自动设置好了对方（收信人）的电子邮件地址和我们自己的电子邮件地址，我们只要写上内容，单击“发送”即可。

这里，关键的是我们在使用 Outlook 前，先要对它进行设置，即 Outlook 账户设置，如没有设置过，自然不能使用。设置的内容是我们注册的网站电子邮箱服务器及账户名和密码等信息。设置时，其设置内容同时也进入了 Office 软件的 Microsoft Outlook 程序账户中。下面，我们简单地介绍设置的过程。

首先，启动 Outlook，从菜单中选择“工具”→“账号”命令，打开“Internet 账号”窗口，如图 16-16 所示。

在图 16-16 中，单击“邮件”标签（默认），然后再单击“添加”按钮，从弹出的菜单中选择“邮件”选项将弹出 Internet 连接向导，如图 16-17 所示。

在图 16-17 中，首先输入我们的“显示姓名”，此姓名将出现在所发送邮件的“寄件人”一栏。然后，单击“下一步”按钮，在弹出的窗口中输入我们的电子邮件邮箱地址，在接收服务器框中，输入邮箱的 POP3 服务器名称（例如 pop.csai.cn）。再单击“下一步”按钮，在弹出的“电子邮件服务器名”窗口中，系统默认“我的接收邮件服务器”为 POP3，不需要修改。

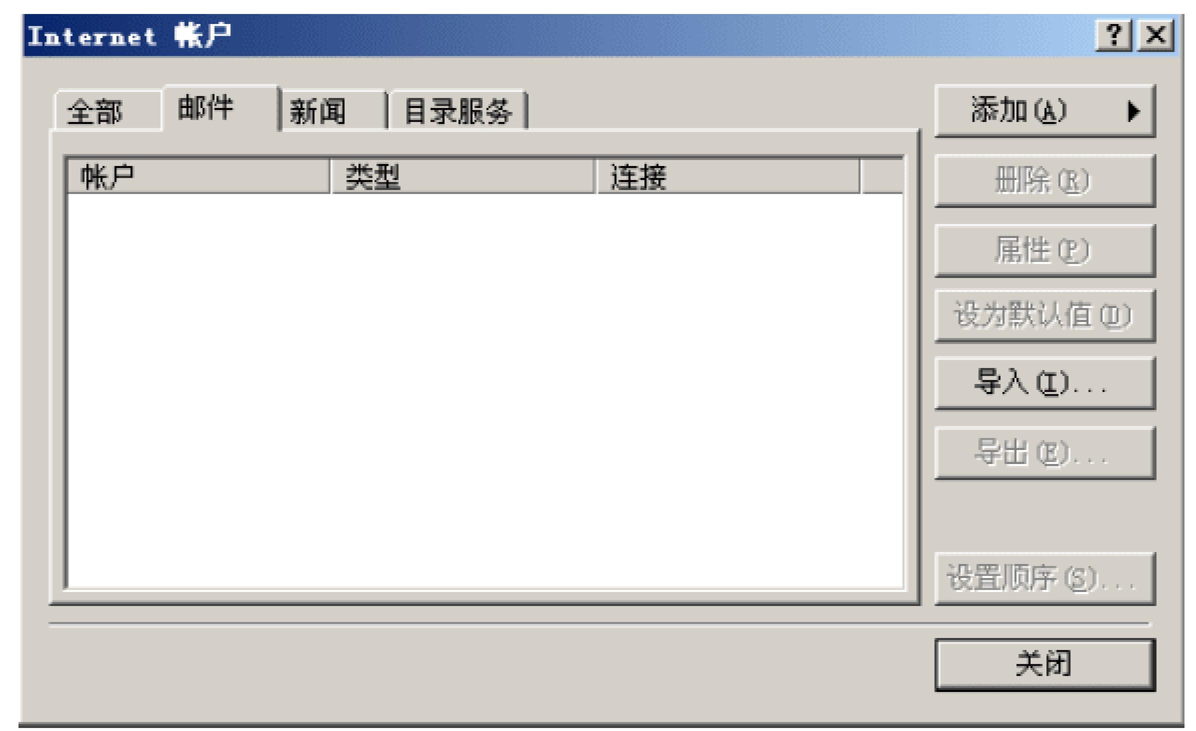


图 16-16　Internet 账号设置



图 16-17　Internet 连接向导

这样，就完成了 Outlook 的初步设置，可以用来收发邮件了。

16.5　例题分析

为了帮助考生更好地理解和掌握本章中的知识点，本节准备了 5 道例题，考生可认真完成例题，体会例题分析，巩固所学知识。

例题 1

在 Windows 系统中，如果用户要整理 D 盘上的碎片，可选中 D 盘，__（1）__，单击“开始整理”按钮，在弹出的对话框中单击“碎片整理”按钮即可；通过设置文件的__（2）__，可以使其成为“隐藏”文件。

（1）A. 双击鼠标左键，选择“属性”对话框中的“常规”选项卡
　　B. 单击鼠标右键，选择“属性”对话框中的“常规”选项卡
　　C. 双击鼠标左键，选择“属性”对话框中的“工具”选项卡
　　D. 单击鼠标右键，选择“属性”对话框中的“工具”选项卡

（2）A. 类型　　B. 格式　　C. 属性　　D. 状态

例题 1 分析

本题主要考察 Windows 系统的文件处理，在 Windows 系统文件设置文件是否隐藏是属于文件属性，可以通过设置文件属性。Windows 系统中碎片的整理可以通过好几种途径，其中一种是选中 D 盘，然后单击鼠标右键，选择“属性”对话框中的“工具”选项卡通过“磁盘整理碎片程序”来实现的。

例题 1 答案

（1）D　　（2）C

例题 2

在 Word 编辑状态下，将正文中所有“internet explorer”改写为“Internet Explorer”，

常选用编辑子菜单上的__（3）__命令；单击“工具”栏中的“__（4）__”按钮可以在光标所在处插入超链接。

（3）A.“修订”　　B.“替换”　　C.“定位”　　D.“粘贴”

（4）A.　　B.　　C.　　D.

例题 2 分析

本题主要考察 Word 的基本操作：替换和超链接，在 Word 中将正文中的文件进行改写可以采用多种方法，其中比较快捷的是替换，可以选择“编辑”菜单下的“替换”命令，或者用快捷键 Ctrl+H，可以弹出“查找和替换”对话框。

在查找内容内填写需要替换的内容，如本题中是 internet explorer，在替换为框内填写替换成为的内容，如本题是 Internet Explorer，还有高级选项，如图 16-18 所示。



图 16-18　查找替换对话框高级选项

如本题就要区分大小写，需要选上，还有格式和特殊字符选项，可以根据具体情况进行选择。替换可以逐个替换，单击对话框中的“替换”按钮，也可以一次性全部替换，单击对话框中的“全部替换”按钮，如果不想替换，单击取消即可。

超链接就是单击链接就自动转换到需要链接的地方，可以是互联网，也可以是一个文件等，在 Word 中设置超链接主要有三种方法，一种是选中需要链接的字符，在“插入”菜单下选择“超链接”，第二种是在工具栏上单击按钮，第三种是单击鼠标右键，弹出一个快捷菜单，选择“超链接”也可。

例题 2 答案

（3）B　　（4）A

例题 3

在 Excel 表处理软件中，__（5）__是公式在复制和移动时会根据移动的位置自动调节公式中引用单元格的地址。假设单元格 A1、A2、B1 和 B2 的内容如图 16-19 所示。并在 C1 中输入公式 “=$ A$1+ B1”，并将公式复制到 C2，那么 C2 的内容为__（6）__。

	A	B	C
1	101	1	
2	102	2	
3			

图 16-19　单元格的内容

（5）A. 绝对引用　　B. 相对引用　　C. 逻辑引用　　D. 物理引用

（6）A. 102　　B. 103　　C. 104　　D. 203

例题 3 分析

在公式中引用单元格或者区域时，引用的类型可分为以下三种：

相对引用：当把公式复制到其他单元格中时，行或列的引用会改变。所谓行或列的引用会改变，即指代表行的数字和代表列的字母会根据实际的偏移量相应改变。

绝对引用：当把公式复制到其他单元格中时，行和列的引用不会改变。（直接复制公式）

混合引用：行或列中有一个是相对引用，另一个是绝对引用。

例题 3 答案

（5）B　　（6）A

例题 4

Excel 学生成绩表如下表所示，若要计算表中每个学生计算机文化和英语课的平均成绩，那么，可通过在 D3 单元格中填写__（7）__，并__（8）__拖动填充柄至 D10 单元格，则可自动算出这些学生的平均成绩。

表 16-1　Excel 学生成绩表

	A	**B**	**C**	**D**
1	学生成绩表			
2	姓名	计算机文化	英语	平均成绩
3	朱小梅	80	76	
4	于　洋	85	72	
5	赵玲玲	90	82	
6	冯　刚	91	79	
7	郑　丽	86	78	
8	孟晓珊	82	76	
9	杨子健	96	86	
10	廖　东	93	80	

（7）A. =AVG(B3+C3)　　B. =AVERAGE(B3+C3)

C. =AVG(B3/C3)　　D. =AVERAGE(B3:C3)

（8）A. 向垂直方向　　B. 向水平方向

C. 按住 Shift 键向垂直方向　　　　D. 按住 Shift 键向水平方向

例题 4 分析

本题考察的 Excel 的公式计算和快捷键的使用。Excel 中计算平均值的公式为 AVERAGE，而不是 AVG，并且 AVERAGE 后面的括号中一般是用分号“：”隔开，表示范围，而不是采用“+”和“/”。由于要计算每个学生的平均值，按照 Excel 的规则，在 Excel 中有规律数据可以进行快速填充，灵活地使用自动填充功能可以避免重复输入数据。若用户需要对某个 Excel 工作表的 D3：D10 的区域快速计算平均成绩，可以采用的方法是在 D3 单元格填入"=AVERAGE(B3:C3)"，并将鼠标移到 E3 单元格的右下角，此时，则可自动算出这些学生的平均成绩，用户向垂平方向拖动填充柄（图中会显示十字光标）至 D10 单元格。

例题 4 答案

（7）D　　　（8）A

例题 5

在 Outlook 中，通常借助__（9）__来传送一个文件。

（9）A．邮件正文　　B．Telnet　　C．WWW　　D．附件功能

例题 5 分析

本题主要考察 Outlook 的使用。在 Outlook 中如果要传送一个文件，如果需要给邮件添加附件，单击工具栏中的“附件”按钮，在“插入附件”窗口中选择你要插入的文件，就可以发送邮件了。

例题 5 答案

（9）D

主要参考文献

[1] 谢希仁．计算机网络（第 5 版）．北京：电子工业出版社，2008.1

[2] 桂阳．网络管理员考试考前串讲. 北京：电子工业出版社，2008.9

[3] 唐平．网络工程师考试考前串讲. 北京：电子工业出版社，2008.9

[4] 徐锋．网络管理员考试冲刺指南. 北京：电子工业出版社，2005.9

[5] 张国鸣．网络管理员教程．北京：清华大学出版社，2004.7

[6] Jim Kurose，Keith ross．计算机网络．北京：清华大学出版社，2002.4

[7] 施游，胡钊源. 网络管理员考试考点分析与真题详解（最新版）．北京：电子工业出版社，2009.3

[8] 雷震甲．网络工程师教程（第 2 版）．北京：清华大学出版社，2006.6

[9] 魏大新，李育龙．Cisco 网络技术教程（第 2 版）．北京：电子工业出版社，2007.4

[10] 徐锋. 网络工程师考试冲刺指南. 北京：电子工业出版社，2005.7

[11] 施游，胡钊源. 网络工程师考试试题分类精解（第 3 版）．北京：电子工业出版社，2009.4

[12] 唐平，张友生. 网络工程师考试考点分析与例题精解．西安：电子科技大学出版社，2008.3